The HIPAA-Pota-Mess: How HIPAA's Weak Enforcement Standards Have Led States To Create Confusing Medical Privacy Remedies

MORGAN LEIGH TENDAM*

TABLE OF CONTENTS

---

* J.D. Candidate, May 2018, The Ohio State University Moritz College of Law. The author would like to thank her mother, Amber Tendam, for being a constant source of inspiration, strength, love, and wisdom throughout law school and life in general, and her grandfather, Charles Barker, for always helping her to chase her dreams. She would also like to thank Danny Skubak for helping her keep her sanity intact throughout law school. Additionally, she would like to thank Professor Efthimios Parasidis for his advice regarding this Note, the entire staff of the *Ohio State Law Journal*, and Gabby Colavecchio for her wonderful guidance and help throughout editing this Note.

I. INTRODUCTION

In 2012, Anita Chanko turned on her television to watch "NY Med," a medical show featuring her city's hospital.[1] Rather than seeing other families' stories, however, she saw footage of her now-deceased husband as a "blurred-out man moaning in pain."[2] Her husband died in April 2011 at the featured hospital after being hit by a truck.[3] Fists clenched and mouth dry, she watched his failed treatment and death all over again.[4] Shockingly, "[t]his was the first time [she] became aware of the recording of [her husband's] medical treatment and death."[5] While the hospital did not believe it violated the Health Insurance Portability and Accountability Act's Privacy Rule, federal regulators and a New York Supreme Court judge disagreed.[6] The hospital will pay $2.2 million in penalties to the federal government for the violation,[7] and because Mrs. Chanko lives in New York, she can also sue the hospital for breaching physician–patient confidentiality.[8] None of the $2.2 million penalty, however, will go to Mrs. Chanko.[9] Her private remedy is separate from the federal settlement payment.

---

[1] Charles Ornstein, *Dying in the E.R., and on TV Without His Family's Consent*, N.Y. TIMES (Jan. 2, 2015), http://www.nytimes.com/2015/01/04/nyregion/dying-in-the-er-and-on-tv-without-his-familys-consent.html (on file with *Ohio State Law Journal*).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Chanko v. Am. Broad. Cos., 49 N.E.3d 1171, 1174 (N.Y. 2016).

[6] Ornstein, *supra* note 1.

[7] Charles Ornstein, *New York Hospital To Pay $2.2 Million over Unauthorized Filming of 2 Patients*, N.Y. TIMES (Apr. 21, 2016), https://www.nytimes.com/2016/04/22/nyregion/new-york-hospital-to-pay-fine-over-unauthorized-filming-of-2-patients.html (on file with *Ohio State Law Journal*).

[8] *Chanko*, 49 N.E.3d at 1178.

[9] *See* Ornstein, *supra* note 7.

The Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)[10] and its Privacy Rule were intended to improve medical privacy. Under these rules, covered entities (generally medical providers)[11] must meet certain requirements and obtain consent before releasing personally identifiable health information.[12] These provisions reflect congressional consensus that: 1) medical privacy is an important right that is crucial for effective medical treatment, and 2) with the proliferation of electronic records and other means of communication, the risk for unauthorized disclosure of private medical information has increased.[13]

HIPAA violations are not met with damages for victims, but rather with penalties paid to the federal government.[14] Without a private right of action, HIPAA leaves victims without recovery and does not properly incentivize covered entities to fully comply, as shown by continued HIPAA violations.[15] In response to this lack of protection, many states apply a confusing and contradictory array of state-based legal doctrines for recovery.[16] These range from negligence suits against those who violate medical privacy standards,[17] to state statutes providing damages,[18] and many things in between.[19] The remaining question, however, is where HIPAA fits within these state-based legal doctrines. HIPAA contains preemption provisions for laws contrary to its requirements (excluding more stringent laws),[20] but which state approaches are actually contrary to HIPAA is unclear. Lower courts are divided on this question, meaning HIPAA is interpreted differently among the states.[21]

This Note explores these questions and disparities, and urges a tort-based solution. In Part II, this Note will discuss HIPAA and its importance. It will also

---

[10] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1, 110 Stat. 1936 (codified at 42 U.S.C. §§ 1320d–1320d-9).

[11] As well as others, which will be examined *infra* Part II.C.

[12] *See infra* Part II.C.

[13] *See Protecting Our Personal Health Information: Privacy in the Electronic Age: Hearings on Examining Standards with Respect to the Privacy of Individually Identifiable Health Information. Views Received from the Secretary, Department of Health and Human Services, Witnesses Representing Consumers Groups, Health Plans, Health Care Providers, Health Professionals, and Researchers Before the S. Comm. on Labor & Human Res.*, 105th Cong. 2–5 (1997) (statements of Sen. Bill Frist, Member, S. Comm. on Labor & Human Res., and Donna E. Shalala, Secretary, U.S. Department of Health and Human Services).

[14] *See* 45 C.F.R. § 160.424(a) (2016) (noting that penalties are collected by the Health and Human Services Secretary).

[15] *See infra* Part III.B.

[16] *See infra* Part IV.B.

[17] *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 36 (Conn. 2014).

[18] *See, e.g.*, CAL. CIV. CODE § 56.35 (West 2007).

[19] *See infra* Part IV.B.

[20] 45 C.F.R. § 160.203(b) (2016); *see also* 42 U.S.C. § 1320d-7(a) (2012).

[21] *See infra* Parts IV.B.2, V.A. For example, in Connecticut, HIPAA informs the standard of care for negligence, but in Ohio, it does not. *See* Sheldon v. Kettering Health Network, 40 N.E.3d 661, 675–76 (Ohio Ct. App. 2015).

discuss how technological advances and unauthorized disclosures threaten the crucial right to medical privacy. Part III argues that HIPAA's current enforcement scheme does not go far enough to protect medical privacy or provide adequate remedies to victims of HIPAA violations.

Part IV examines state approaches to HIPAA enforcement and whether the Act's language preempts state causes of action. Part V presents a two-pronged solution. First, it advocates for an independent tort approach similar to Ohio's treatment of medical privacy violations, but with suggested modifications. Second, this Note argues that because Congress has been unwilling to address HIPAA's preemption and remedy problems and appellate courts have answered the problem in conflicting ways, a definitive opinion from the Supreme Court is needed to clarify the strength and reach of HIPAA's enforcement scheme. Finally, Part VI concludes by linking the importance of medical privacy to the proposed independent tort approach and need for Supreme Court guidance, which will help protect sensitive information where others have so far failed.

II. WHAT IS HIPAA AND WHY DOES IT MATTER SO MUCH?

Medical privacy is both a historic and modern concept. Long ago, Hippocrates penned the Hippocratic Oath: "Whatever, in connection with my professional practice, or not in connection with it, I see or hear in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."[22] While some modern physicians think this should be "radically modified," or "abandoned altogether" because of its antiquity,[23] the legal controversy surrounding medical privacy today shows this is an important, changing, and serious issue. Recognizing, in part, the importance of medical privacy, Congress passed HIPAA in 1996.[24]

In modern society, where medical information can be shared at the click of a button and medical records include everything from genetic data to sexual activity, medical privacy is incredibly important. Congress sought to protect this information through HIPAA and its implementing regulations and rules, which specify when information can be shared and the penalties for unauthorized disclosures.[25]

---

[22] MARGARET BRAZIER & EMMA CAVE, MEDICINE, PATIENTS AND THE LAW 83 (5th ed. 2011); Peter Tyson, *The Hippocratic Oath Today*, PBS (Mar. 27, 2001), http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html [https://perma.cc/DQ7Q-2WF4] (noting that Hippocrates lived early in the 5th Century, B.C., but also that the oath's origins are unknown).

[23] *See* Tyson, *supra* note 22.

[24] *See Confidentiality of Patient Records: Hearing Before the Subcomm. on Health of the H. Comm. on Ways & Means*, 106th Cong. 2 (2000) [hereinafter *Confidentiality Hearing*].

[25] *See id.*

A. *The Importance of Medical Privacy*

Medical privacy is important for both our healthcare system and for individuals. First, Congress recognized that without medical privacy, the public lacks "confidence in our health care system."[26] When patients lack confidence, they might delay treatment or lie to doctors, which can increase "personal and financial costs" and result in a "decline in [overall] societal health."[27]

Second, medical records "strip us naked" by revealing very sensitive, personal information, which can negatively impact lives when disclosed.[28] "Individually identifiable health information" broadly refers to anything relating "to the past, present, or future physical or mental health or condition of an individual,"[29] and includes "financial and billing information, . . . sexually transmitted diseases, contraception, abortion, substance abuse problems, mental illness, and medications."[30] Without protections, employers and insurance companies could abuse medical records to harass or discriminate against patients.[31] Many who have suffered from potential improper disclosures[32] experience "personal embarrassment or harm" and worry that disclosures to family members, employers, or friends might "negatively impact their job

---

[26] *Id.* at 6 (statement of Rep. William M. Thomas, Chairman, Subcomm. on Health, H. Comm. on Ways & Means); *see id.* (statement of Rep. Jim McDermott, Member, Subcomm. on Health, H. Comm. on Ways & Means) ("If you do not trust the physician, or the nurse or whoever the health provider is that this information is going to be kept private, you are liable to withhold or tell only half the story or whatever.").

[27] *Id.* at 10 (statement of Rep. Jim McDermott, Member, Subcomm. on Health, H. Comm. on Ways & Means).

[28] *See* Ralph Ruebner & Leslie Ann Reis, *Hippocrates to HIPAA: A Foundation for a Federal Physician-Patient Privilege*, 77 TEMP. L. REV. 505, 512 (2004) (quoting SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 125 (Deborah Russell ed., 2000)) (discussing medical privacy in the context of a federal physician–patient privilege). While the Ruebner & Reis article largely focuses on the federal physician–patient privilege, the information about medical privacy itself is relevant in both the privilege and more general medical privacy suit contexts. *See id.* Such a privilege would also protect individuals' medical privacy. *See id.* at 519–20.

[29] 45 C.F.R. § 160.103 (2016) (defining health information under HIPAA).

[30] Ruebner & Reis, *supra* note 28, at 517.

[31] *See id.* at 527–28.

[32] This includes actual disclosures as well as potential disclosures because personal harm encompasses both actual embarrassment and damage, as well as harm from worrying that information may have been leaked and the potential effects from that.

security, relationships, or personal safety."[33] In the face of new technology, these fears are becoming even more heightened.[34]

Today, almost no one is immune from improper personal information disclosures.[35] From an Indiana woman's human papillomavirus diagnosis being spread on Facebook by a local hospital technician[36] to Farrah Fawcett discovering a hospital employee sold her cancer diagnosis information to

---

[33] Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y L. & ETHICS 327, 329 (2002). The risk of disclosure can also cause isolation and discrimination by employers. Joshua D.W. Collins, Note, *Toothless HIPAA: Searching for a Private Right of Action To Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 201 (2007). Prior to the Affordable Care Act's guaranteed coverage for preexisting conditions, there was also concern that improper disclosures could lead to insurance denials. *See id.*

[34] While electronic health care has increased speed, flexibility, and communication within medicine, it also creates risks for patients. Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 332 (2007). Once health "data is dispersed on the Internet, it becomes available to anyone who is willing to pay for it, and it cannot be expunged." *Id.* at 335 (footnote omitted). New types of healthcare data are also at risk, like genetic testing, which reveals a massive amount of sensitive information about individuals. *See* Ruebner & Reis, *supra* note 28, at 520–21; Charles Ornstein, *Federal Privacy Law Lags Far Behind Personal-Health Technologies*, WASH. POST (Nov. 17, 2015), https://www.washingtonpost.com/news/to-your-health/wp/2015/11/17/federal-privacy-law-lags-far-behind-personal-health-technologies/ [https://perma.cc/52FL-ENMH] ("At-home paternity tests fall outside the law's purview. For that matter, so do wearables like Fitbit that measure steps and sleep, gene testing companies like 23andMe, and online repositories where individuals can store their health records."). Furthermore, because doctors are now encouraged by the "movement toward electronic storage of medical information" to increase the amount of information they collect from patients, things like lifestyle choices, sexual orientation, and diagnoses are inside electronic records. Ruebner & Reis, *supra* note 28, at 521. Hackers can also access social security numbers, causing huge amounts of "financial and emotional stress" to victims "wondering if and when [their] information will be used against them." Austin Rutherford, Comment, Byrne: *Closing the Gap Between HIPAA and Patient Privacy*, 53 SAN DIEGO L. REV. 201, 202 (2016) (discussing the hack of health insurer Anthem, where hackers accessed the social security numbers and other personal information of "over eighty million people[]").

[35] *See* Charles Ornstein, *Your Health Records Are Supposed To Be Private. They Aren't.*, WASH. POST (Dec. 30, 2015), https://www.washingtonpost.com/posteverything/wp/2015/12/30/your-health-records-are-supposed-to-be-private-they-arent/ [https://perma.cc/P8MV-LPYM].

[36] Charles Ornstein, *Small-Scale Violations of Medical Privacy Often Cause the Most Harm*, PROPUBLICA (Dec. 10, 2015) [hereinafter Ornstein, *Small-Scale Violations*], https://www.propublica.org/article/small-scale-violations-of-medical-privacy-often-cause-the-most-harm [https://perma.cc/TDT7-XF3X]. The victim's full name, diagnosis, and birthdate were posted on Facebook by the technician, who attended the victim's high school. *Id.* The post included statements like "PPL WORLD WIDE, . . . FRANCES . . . IS HPV POSITIVE," and "PLZ HELP EXPOSE THIS HOE!" *Id.*

tabloids,[37] medical privacy violations can affect almost anyone.[38] Society recognizes this danger as well. A 2013 study showed that around 60% of American adults were "very or somewhat concerned about unauthorized viewing when their medical records are sent electronically between health care providers."[39] While patients recognize the benefits of electronic health records, they are aware of the very realistic risks.[40]

B. *HIPAA: The Congressional Solution to Medical Privacy*

In light of increasing concerns about medical privacy, in 1996 Congress took the historic step of enacting HIPAA.[41] One of Congress's main purposes in enacting HIPAA was protecting health information security.[42] HIPAA's Privacy Rule, which "establish[ed] national standards to protect individuals' medical records and other personal health information," was promulgated in its final form in 2002.[43] In essence, HIPAA restricts how doctors and other entities can release information, but also creates specific instances where medical information may be disclosed without patient authorization.[44] Prior to HIPAA,

---

[37] Ornstein, *supra* note 35.

[38] For more examples of intrusion into and release of sensitive information, see Daniel J. Oates, Comment, *HIPAA Hypocrisy and the Case for Enforcing Federal Privacy Standards Under State Law*, 30 SEATTLE U. L. REV. 745, 745–46 (2007).

[39] VAISHALI PATEL ET AL., THE OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., INDIVIDUALS' PERCEPTIONS OF THE PRIVACY AND SECURITY OF MEDICAL RECORDS 3 (June 2015), https://www.healthit.gov/sites/default/files/briefs/oncdatabrief27june2015privacyandsecurity.pdf [https://perma.cc/KQ4R-D2TE]. These results are largely the same between those with paper and electronic medical records, although those with electronic records had "slightly higher rates of withholding information from their provider due to privacy or security concerns." *Id.* at 2.

[40] *Id.* at 5.

[41] U.S. Dep't of Health & Human Servs., *HIPAA for Professionals*, HHS.GOV [hereinafter HHS, *HIPAA for Professionals*], https://www.hhs.gov/hipaa/for-professionals/ [https://perma.cc/TA8W-43X3] (last reviewed June 16, 2017).

[42] C. STEPHEN REDHEAD, CONG. RESEARCH SERV., MEDICAL RECORDS PRIVACY: QUESTIONS AND ANSWERS ON THE HIPAA FINAL RULE 2 (Oct. 2002), https://digital.library.unt.edu/ark:/67531/metacrs2251/m1/1/high_res_d/RS20500_2002Oct03.pdf [https://perma.cc/YY9J-Y8JB] (listing reasons included reducing paperwork, lowering administrative causes, and coordinating health care information and activities). Especially in the face of new technology, Congress realized new threats "could erode the privacy of health information." HHS, *HIPAA for Professionals*, *supra* note 41. Thus, Congress added standards to protect "individually identifiable health information" on a federal level. *Id.*

[43] U.S. Dep't of Health & Human Servs., *The HIPAA Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/ [https://perma.cc/V3B3-GWJ9] (last reviewed Apr. 16, 2015).

[44] REDHEAD, *supra* note 42, at 2–3. In sum, Congress was responding to growing concerns about medical privacy when it enacted HIPAA. *See id.* at 2. The protections it provided were a new and seemingly important expansion of federal law to protect important rights, but they also generated confusion and criticism. *See* Luke Gale, *HIPAA at 20: Looking Back at Two Decades of Patient Privacy Protections*, HEALTHCARE DIVE (Aug. 30, 2016),

no federal laws regulated medical privacy.[45] Thus, "for the first time, a set of basic national privacy standards and fair information practices . . . provide[d] all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care."[46] HIPAA's actual operation, however, is governed by the Privacy Rule.[47]

C. *HIPAA in Action: How HIPAA Protects Personal Health Information*[48]

HIPAA's Privacy Rule prohibits covered entities,[49] such as doctors or hospitals, from using or disclosing "protected health information" (PHI) without a "valid authorization."[50] Even with a valid authorization, the law mandates that disclosures must be consistent with the authorization.[51] PHI includes

---

http://www.healthcaredive.com/news/hipaa-at-20-looking-back-at-two-decades-of-patient-privacy-protections/425378/ [https://perma.cc/PHP4-DZZT] ("While patients are technically afforded the right under HIPAA to access their own personal health information, . . . third parties often have more access to [anonymized] personal health information than patients themselves.").

[45] Daniel J. Solove, *HIPAA Turns 10: Analyzing the Past, Present and Future Impact*, AHIMA (Apr. 2013), http://library.ahima.org/doc?oid=106325 [https://perma.cc/SM7N-6YPP]. Before HIPAA, states were the "primary regulators of health information through their constitutions, common law, and statutory provisions." Pritts, *supra* note 33, at 327.

[46] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164) [hereinafter Standards for Privacy].

[47] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 164) [hereinafter Standards 2002]. The HIPAA privacy regulations, which define terms and further set out HIPAA rules, are promulgated by the Secretary of the Department of Health and Human Services. *See* 42 U.S.C. §§ 1320d–1320d-9 (2012).

[48] This Note focuses only on the Privacy Rule, not HIPAA's other rules which could potentially carry their own torts and other implications.

[49] Covered entities include health plans, health care clearinghouses, and "health care provider[s] who transmit[] any health information in electronic form in connection with a transaction covered" by the federal regulations implementing HIPAA. 45 C.F.R. § 160.102(a)(1)–(3) (2016). Covered entities can also include "business associates." *Id.* § 160.102(b). In general, these are "person[s] or entit[ies] that perform[] certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provide[] services to, a covered entity," but not including a "covered entity's workforce." U.S. Dep't of Health & Human Servs., *Business Associates*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [https://perma.cc/NG9P-WA8C] (last reviewed July 26, 2013); *see also* 45 C.F.R. § 160.103. The Privacy Rule standards "apply to covered entities with respect to protected health information." 45 C.F.R. § 164.500(a) (2015).

[50] 45 C.F.R. § 164.502(a)(1)(iv) (2015).

[51] *Id.* § 164.508(a). A "valid authorization under this section must contain at least" 1) a "specific and meaningful" description of what information is being used/disclosed, 2) "[t]he name or other specific identification of the person(s) . . . authorized to make the requested use or disclosure," 3) the names or identities of the person(s) "to whom the covered entity

individually identifiable health information[52] that is "(i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium."[53] For example, PHI can include both information in individuals' medical charts[54] and their genetic information.[55] The Privacy Rule lays out specific allowed uses and disclosures for PHI.[56] For example, a covered entity can disclose PHI to the individual it is about when the individual requests it,[57] or "for treatment, payment, or [other] health care operations."[58] Covered entities may also disclose information about reasonably suspected abuse or domestic violence to government authorities, such as protective service agencies.[59] While on its face complex and comprehensive, HIPAA has not adequately protected patient privacy due to lax and inconsistent enforcement.

III. HIPAA INACTION: HOW IT IS ENFORCED AND WHY THIS IS NOT ENOUGH

While HIPAA's Privacy Rule strives to protect privacy rights, lax enforcement has led to serious concerns about the rule's strength, stringency, and effectiveness.[60] As enforcement agencies continue to favor voluntary compliance over penalties and sanctions,[61] victims of medical privacy violations

---

may make the requested use or disclosure," 4) "[a] description of each purpose of the requested use or disclosure," 5) the expiration date or event on which the disclosure/authorization ends, and 6) the individual's signature and the date. *Id.* § 164.508(c)(i)–(vi).

[52] The regulations define "individually identifiable health information" as "information that is a subset of health information, including demographic information collected from an individual" that is "created or received by a health care provider, health plan, employer, or health care clearinghouse" that also "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual" and either "identifies the individual" or creates "a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103 (2016).

[53] *Id.*

[54] U.S. Dep't of Health & Human Servs., *Your Rights Under HIPAA*, HHS.GOV [hereinafter HHS, *Your Rights Under HIPAA*], https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html [https://perma.cc/TNX3-CZGV] (last reviewed Feb. 1, 2017).

[55] U.S. Dep't of Health & Human Servs., *Does the HIPAA Privacy Rule Protect Genetic Information?*, HHS.GOV (Dec. 20, 2002), https://www.hhs.gov/hipaa/for-professionals/faq/354/does-hipaa-protect-genetic-information/index.html [https://perma.cc/HLU4-LWU9].

[56] *See* 45 C.F.R. §§ 164.502–164.526 (2015).

[57] *Id.* § 164.502(a)(1)(i), (a)(2)(i).

[58] *Id.* § 164.506(a).

[59] *Id.* § 164.512(c)(1).

[60] *See infra* Part III.B.

[61] *See infra* notes 65–67 and accompanying text.

are left without personal remedies for their often stigmatizing and personally devastating harms.

A. *HIPAA Enforcement Procedures*

If an individual's medical privacy rights are violated under the Privacy Rule, that person cannot directly sue the guilty party.[62] Instead, victims must file their complaints with the Health and Human Services (HHS) Secretary through the Office for Civil Rights (OCR),[63] or seek relief through their state attorney general.[64] The OCR can investigate complaints, "conduct compliance reviews," and "perform[] education and outreach to foster compliance" with the Privacy Rule.[65] After an investigation, the OCR must decide whether the complaint should be sent to the Department of Justice (DOJ) for criminal investigations.[66] If the OCR determines that the covered entity violated HIPAA's Privacy Rule, it can try to solve the issue "by obtaining[] [v]oluntary compliance[,] [c]orrective action[,] and/or [r]esolution agreement[s]."[67]

---

[62] Jack Brill, Note, *Giving HIPAA Enforcement Room To Grow: Why There Should Not (Yet) Be a Private Cause of Action*, 83 NOTRE DAME L. REV. 2105, 2106 (2008); *see, e.g.*, Sneed v. Pan Am. Hosp., 370 F. App'x 47, 50 (11th Cir. 2010) (per curiam) ("We decline to hold that HIPAA creates a private cause of action . . . ."); Adams v. Eureka Fire Prot. Dist., 352 F. App'x 137, 139 (8th Cir. 2009) (per curiam) ("HIPAA does not create a private right . . . .").

[63] *See* 45 C.F.R. § 160.306(a) (2016); *see also* U.S. Dep't of Health & Human Servs., *What OCR Considers During Intake & Review*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/what-OCR-considers-during-intake-and-review/index.html [https://perma.cc/5APR-W5TF] (last reviewed June 7, 2017). While the OCR is involved in many areas of government services, in the HIPAA/medical privacy context, its mission is to "protect[] [individuals'] fundamental nondiscrimination and health information privacy rights." U.S. Dep't of Health & Human Servs., Office for Civil Rights, *About Us*, HHS.GOV, https://www.hhs.gov/ocr/about-us/index.html [https://perma.cc/BE4Q-WUER] (last reviewed Sept. 6, 2015).

[64] 42 U.S.C. § 1320d-5(d)(1)–(2) (2012).

[65] U.S. Dep't of Health & Human Servs., *How OCR Enforces the HIPAA Privacy & Security Rules*, HHS.GOV [hereinafter HHS, *How OCR Enforces*], https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html [https://perma.cc/Z9A6-9XXV] (last reviewed June 7, 2017).

[66] *Id.*

[67] *Id.* These are the most common enforcement methods. *Id.* One example of voluntary compliance measures, instead of compulsory punishments, revolves around the improper disclosure of Peter Brabeck's information in California. *See* Ornstein, *Small-Scale Violations*, *supra* note 36. Peter's doctor allegedly overprescribed Peter controlled substances without an examination, resulting in a medical board investigation of the doctor. *Id.* The doctor hired a private investigator to investigate Peter, and gave him access to "all of [Peter's] medical records." *Id.* After the doctor refused to pay him, the investigator offered to sell the records to Peter, who then complained to OCR. *Id.* After two years, the OCR claimed the complaint was resolved because the clinic was given "guidance on how to comply with privacy rules" and the doctor agreed to apologize, acknowledge his improper

Unauthorized disclosures of individually identifiable health information can also result in penalties and potential jail sentences.[68] However, monetary penalties go to the U.S. Treasury rather than to the victims.[69] In sum, while there are processes for filing complaints, "a patient who has been seriously harmed as a result of . . . privacy leaks cannot bring a lawsuit against the responsible party" or recover individually, and instead must rely on a government penalty and enforcement process.[70]

B. *HIPAA's Enforcement Procedures Alone Do Not Adequately Protect Patient Privacy*

As many have noted, HHS rarely imposes fines/sanctions, and victims are not compensated for the harm caused by improper disclosures.[71] Recently, OCR Director Jocelyn Samuels noted that the agency's "preference is always to promote voluntary compliance."[72] Since HIPAA lacks a private right of action, for the patients harmed in these cases, the OCR/HHS is often "the only place they can seek vindication."[73] As such, in 2015, HHS received 17,643 complaints,[74] but 72% were resolved after intake and review and only 4%

---

disclosure, and give Peter free credit monitoring. *Id.* Peter stated he has not received any of these. *Id.* There were no monetary or other penalties. *See id.*

[68] 42 U.S.C. § 1320d-6(a)–(b).

[69] *See* 45 C.F.R. § 160.424(a) (2016); *see also* HHS, *How OCR Enforces*, *supra* note 65.

[70] Collins, *supra* note 33, at 201–02.

[71] *Id.* at 202; *see also* Oates, *supra* note 38, at 750–52. In 2015, after studying breaches of protected health information, the Office of the Inspector General recommended "OCR should strengthen its followup of breaches of PHI reported by covered entities." SUZANNE MURRIN, DEP'T OF HEALTH & HUMAN SERVS., OFFICE OF INSPECTOR GEN., OCR SHOULD STRENGTHEN ITS FOLLOWUP OF BREACHES OF PATIENT HEALTH INFORMATION REPORTED BY COVERED ENTITIES 13 (Sept. 2015), https://oig.hhs.gov/oei/reports/oei-09-10-00511.pdf [https://perma.cc/A4QP-8CEC].

[72] Ornstein, *Small-Scale Violations*, *supra* note 36. There are relatively few criminal HIPAA prosecutions in the United States. For example, a case out of Anchorage, Alaska in 2015 was one of the first in the state and "one of the few in the country." Press Release, U.S. Dep't of Justice, Anchorage Woman Sentenced to Two Years Imprisonment for HIPAA Violation (June 1, 2015), https://www.justice.gov/usao-ak/pr/anchorage-woman-sentenced-two-years-imprisonment-hipaa-violation [https://perma.cc/H5F7-MD5E]. There, Stacy Laulu was convicted of two felony HIPAA violations and sentenced to two years in jail after using her access to a hospital's medical records to inform her codefendant about his sexual assault and gunshot victims' medical records and other confidential information. *Id.* In sentencing, the judge noted, "in this day and age, every human being expects private records to remain private." *Id.*

[73] Ornstein, *Small-Scale Violations*, *supra* note 36.

[74] U.S. Dep't of Health & Human Servs., *Health Information Privacy Complaints Received by Calendar Year*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html [https://perma.cc/E2HF-QKG8] (last reviewed Oct. 13, 2016).

actually received some type of corrective action.[75] However, even that 4% did not result in victim compensation.

As a result, it is easy to see why HIPAA enforcement is not enough for medical privacy victims. Victims are often left with severe emotional trauma or embarrassment,[76] while covered entities need only, for example, "reposition . . . computer monitors to prevent patients from viewing information on the screens," and apologize to patients.[77] Because of this, many states have struck out on their own to find medical privacy solutions to protect their citizens.

IV. DIFFERENT APPROACHES TO ENFORCING MEDICAL PRIVACY: STATE SOLUTIONS PLUS PREEMPTION AND OTHER PROBLEMS

States have created their own solutions for medical privacy violations, each with its own benefits and downfalls.[78] In assessing each approach, courts generally must decide if the law/action is preempted by HIPAA.[79] Divergent state court interpretations of the same federal statute lead to a clear problem: An individual's medical privacy rights vary between the states.[80] To fix that problem, it is important to first understand preemption in the HIPAA context.

A. *General Statutory HIPAA Preemption*[81]

The Supremacy Clause of the United States Constitution guarantees that federal laws are the "supreme Law of the Land."[82] This means when federal and state laws conflict, federal law preempts or generally controls.[83]

---

[75] U.S. Dep't of Health & Human Servs., *Enforcement Results by Year*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html [https://perma.cc/UGM8-EQAH] (last reviewed Oct. 13, 2016).

[76] *See, e.g.*, Ornstein, *Small-Scale Violations*, *supra* note 36.

[77] *See* U.S. Dep't of Health & Human Servs., *All Case Examples*, HHS.GOV [hereinafter HHS, *All Case Examples*], https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html#case12 [https://perma.cc/M8MT-U3HF] (last reviewed June 7, 2017).

[78] *See infra* Part IV.B.

[79] *See, e.g.*, Murphy v. Dulay, 768 F.3d 1360, 1367–68 (11th Cir. 2014) (performing a preemption analysis on a Florida statute requiring patients attempting to bring medical negligence claims to authorize the release of their protected health information); O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176, 1183–84 (D. Wyo. 2001) (deciding whether HIPAA completely preempts state law claims).

[80] *See infra* Part IV.B.

[81] This Subpart discusses only HIPAA's statutory preemption clause. The preemption problem surrounding HIPAA-based torts, which is the focus of this Note, is more clearly spelled out in Part. IV.B.2.c.i.

[82] U.S. CONST. art. VI.

[83] *See* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 412 (5th ed. 2015). The Supreme Court has recognized three types of federal preemption. *Id.* at 413. First, there is explicit preemption, which occurs when Congress includes explicitly preemptive language. Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 98 (1992)

HIPAA has its own conflict preemption clause, stating that HIPAA generally "supersede[s] any contrary provision of State law."[84] A state law is contrary to HIPAA's Privacy Rule when "[a] covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or [when] [t]he provision of State law stands as an obstacle to the accomplishment and execution" of the Rule's purposes and objectives.[85] However, if the "State law relates to the privacy of individually identifiable health information and is more stringent than" the Privacy Rule, then there is no preemption.[86]

Laws are "more stringent" than the Privacy Rule when they prevent a use or disclosure the Privacy Rule would normally allow.[87] They are also more stringent if they "narrow the scope or duration, increase the privacy protections afforded . . . , or reduce the coercive effect of the circumstances surrounding the express legal permission" of "the form, substance, or . . . need for express legal permission from an individual[] who is the subject of the individually identifiable health information," or "provide[] greater privacy protection for the individual who is the subject of the individually identifiable health information"

(O'Connor, J.). Second, field preemption occurs when "the scheme of federal regulation is 'so pervasive as to make reasonable the inference that Congress left no room for the States to supplement it.'" *Id.* (quoting Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947)). Third, conflict preemption occurs when it is physically impossible to comply with both the state and federal rules/regulations, *id.* (citing Fla. Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142–43 (1963)), or "where state law 'stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress,'" *id.* (quoting Felder v. Casey, 487 U.S. 131, 138 (1988); Perez v. Campbell, 402 U.S. 637, 649 (1971); Hines v. Davidowitz, 312 U.S. 52, 67 (1941)).

[84] 42 U.S.C. § 1320d-7(a)(1) (2012). This includes "a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form." *Id.* State laws include state "constitution[s], statute[s], regulations[s], rule[s], common law, or other State action[s] having the force and effect of law." 45 C.F.R. § 160.202 (2016).

[85] 45 C.F.R. § 160.202.

[86] *Id.* § 160.203(b); *see also* 42 U.S.C. § 1320d-7(a)(2)(B). A law "[r]elates to the privacy of individually identifiable health information" when it specifically protects "health information or affects the privacy of health information in a direct, clear, and substantial way." 45 C.F.R. § 160.202. Also, HIPAA does not supersede contrary provisions that the HHS Secretary determines are necessary for purposes including to "prevent fraud and abuse," to help states regulate "insurance and health plans," to enable "State reporting on health care delivery costs," or that "address[] controlled substances." 42 U.S.C. § 1320d-7(a)(2)(A)(i)–(ii). Contrary state law provisions are also not preempted if they relate to disease, "injury, child abuse, birth, or death" reporting, "or for the conduct of public health surveillance, investigation, or intervention." 45 C.F.R. § 160.203(c). State laws requiring "a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals" are not preempted when contrary to HIPAA as well. *Id.* § 160.203(d).

[87] 45 C.F.R. § 160.202.

regarding all other matters.[88] Thus, HIPAA creates the "federal 'floor' of minimum privacy protections,"[89] and the question courts face regarding medical privacy is whether the state approach is preempted by HIPAA by falling short of the federal floor.[90]

---

[88] *Id.*; *see also* U.S. Dep't of Health & Human Servs., *How Do I Know if a State Law Is "More Stringent" than the HIPAA Privacy Rule?*, HHS.GOV (Mar. 12, 2003) [hereinafter HHS, *More Stringent*], https://www.hhs.gov/hipaa/for-professionals/faq/403/how-do-i-know-if-a-state-law-is-more-stringent-than-hipaa/index.html [https://perma.cc/2ZZ6-64GH] ("For example, a State law that provides individuals with a right to inspect and obtain a copy of their medical records in a more timely manner than the Privacy Rule is 'more stringent' than the Privacy Rule."). When the state law is more stringent than the Privacy Rule, but also contrary to it, the more stringent "State law prevails." *Id.* When the Privacy Rule and more stringent state rule "are not contrary, covered entities must comply with both." *Id.* The regulation contains other conditions marking laws as "more stringent" as well, which are less relevant to this discussion. *See* 45 C.F.R. § 160.202.

[89] REDHEAD, *supra* note 42, at 6. In a hearing about the proposed Privacy Rule, the Assistant Secretary for Planning and Evaluation in HHS noted that HIPAA's confidentiality rules are "cumulative" along with state laws, meaning that HIPAA provides "every American with a basic set of rights with respect to health information." *Confidentiality Hearing*, *supra* note 24, at 18 (statement of Margaret A. Hamburg, Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services). HHS has said that the Congressional goal behind the explicit preemption regulations was "to let the law that is most protective of privacy control (the 'federal floor approach' . . .)." Standards for Privacy, *supra* note 46, at 82,580. However, HHS rejected using the term "most protective of the individual's privacy" in favor of "more stringent" because "more stringent" provided more guidance. *Id.* at 82,582.

[90] *See HIPAA Regulations: Preemption of State Law: Definitions: Contrary - § 160.202*, BRICKER & ECKLER [hereinafter *Preemption of State Law*], http://www.bricker.com/industries-practices/hipaa-health-information-technology/insights-resources/resource/hipaa-regulations-preemption-of-state-law-definitions-contrary-%C2%A7-160202-274 [https://perma.CC/W4UD-SZ7M] ("Since preemption is a judicially developed doctrine, it is reasonable to interpret this term as indicating that the statutory analysis should tie in to the analytical formulations employed by the courts. Also, while the court-developed tests may not be as clear as commenters would like, they represent a long-term, thoughtful consideration of the problem of defining when a state/federal conflict exists. They will also, we assume, generally be employed by the courts when conflict issues arise under the rules . . . .").

B. *Varied State Solutions: The HIPAA-Pota-Mess*[91]

Prior to HIPAA, states were "the primary regulators of health information."[92] When the Privacy Rule was promulgated, HHS noted that "[s]tate laws [were] a crucial means of protecting health information," but they varied "dramatically."[93] Especially regarding "consent for use and disclosure," the existing laws failed to meet public expectations.[94]

Because HIPAA has also failed to meet expectations about protecting privacy due to lax enforcement and standards, states have continued to make, keep, and update their own privacy rules.[95] However, these rules and individuals' medical privacy rights remain varied across state lines.[96] While HIPAA was intended to set national standards and make up for increasingly varied state privacy laws, its lack of enforcement seems to have had the opposite effect.[97]

1. *State Statutes About Medical Privacy*

Some states have created their own statutes addressing medical privacy, which helps patients and providers by setting clear expectations and limits on what can and cannot be done.[98] For example, if a California medical provider improperly discloses medical information without authorization and it is accompanied by either economic loss or personal injury, the victim can recover compensatory damages, punitive damages, attorney's fees, and other litigation costs.[99]However, these state-specific remedies, penalties, punishments, and

---

[91] Prior to HIPAA, "virtually every state ha[d] enacted one or more laws to safeguard privacy." Standards for Privacy, *supra* note 46, at 82,463. Analyzing each possible approach is beyond this Note's scope. Instead, this Note focuses on the dominant approaches and those addressed by the most recent litigation. This Note also focuses on tort-based approaches, as many others have already suggested or analyzed state law and other statutory solutions. *See, e.g.*, Pritts, *supra* note 33, at 327–28 (discussing state statutory solutions); Collins, *supra* note 33, at 208–24 (discussing both 42 U.S.C. § 1983 suits and the False Claims Act).

[92] *See* Pritts, *supra* note 33, at 330.

[93] Standards for Privacy, *supra* note 46, at 82,472.

[94] *See id.* at 82,473.

[95] *See supra* Part III.B; *infra* Part IV.B.2.

[96] *See* Oates, *supra* note 38, at 763.

[97] *See* Standards for Privacy, *supra* note 46, at 82,463–64.

[98] As the Congressional Research Service notes, some states have "detailed, stringent standards governing the use and disclosure of health information," and privacy protections that are stronger than those provided by HIPAA are not preempted. REDHEAD, *supra* note 42, at 6; *see also* Pritts, *supra* note 33, at 335.

[99] *See* CAL. CIV. CODE § 56.35 (West 2007). Texas also has strong privacy protections for its citizens. *See* Peg D. Hall & Matt Nickel, *New Medical Privacy Law in Texas: What You Need To Know*, DALL. B. ASS'N (July 24, 2015), http://www.dallasbar.org/book-page/new-medical-privacy-law-texas-what-you-need-know [https://perma.cc/THC6-UXMC] ("Concerned that HIPAA and HITECH did not provide enough safeguards for protected health information (PHI), the Texas legislature passed H.B. 300 in 2011."). While the statute

sanctions vary across the country and can govern anything from public health to privileged communications, and some even set out provider-specific rules.[100]

Some medical law scholars recommend that since "[s]tates have traditionally been the primary regulators of health care information," in a post-HIPAA world they should continue to be active and enact "statutes that either mirror or build upon the federal protections."[101] Protections going above and beyond HIPAA are likely not preempted; thus, states could continue to create their own rules.[102]

While this seems like a good approach because states could craft rules to avoid HIPAA preemption, this method also has problems. First, as previously noted, these types of statutes and regulations vary greatly.[103] Congress, courts, and individuals have recognized the importance of medical privacy, and having such varied protections is at odds with that.[104] Healthcare providers operating across state lines or patients moving between states will face difficulties adjusting to differing laws, which diminishes uniformity and places value on some protections over others.[105]

As for the preemption analysis, this approach burdens healthcare providers who must "identify[] all state law provisions that affect [their] privacy policies and practices, decide which of those provisions specifically 'relate to' the privacy of individually identifiable health information, and then determine

---

explicitly adopts HIPAA provisions, TEX. HEALTH & SAFETY CODE ANN. § 181.004(a) (Vernon 2010 & Supp. 2015), it also provides some more expansive protections, Hall & Nickel, *supra*. For example, Texas's definition of "covered entities" is more expansive than HIPAA's because it includes all "business associate[s], health care payer[s], governmental unit[s], information or computer management entit[ies], school[s], health researcher[s], health care facilit[ies], clinic[s], health care provider[s], or person[s] who maintain[] an Internet site" and who assemble, collect, analyze, use, evaluate, store, or transmit protected health information "for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis." TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2)(A). It also covers those who "come[] into possession of protected health information[,] . . . obtain[] or store[] protected health information," or are "employee[s], agent[s], or contractor[s]" of the previously listed entities "insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information." *Id.* § 181.001(b)(2)(B)–(D). For more information on the Texas statute, see Hall & Nickel, *supra*.

[100] Pritts, *supra* note 33, at 335–36, 338. "The result of this ad hoc approach is that in many states, there is no statutory guidance as to the proper use and disclosure of health information with respect to many of the major providers of health care." *Id.* at 336.

[101] *Id.* at 347.

[102] *See id.*

[103] *See* Grace Ko, Note, *Partial Preemption Under the Health Insurance Portability and Accountability Act*, 79 S. CAL. L. REV. 497, 505–06 (2006).

[104] *See supra* Parts III.A–B.

[105] *See* Ko, *supra* note 103, at 506 ("Because covered entities must respect the laws of the states in which they do business, they have been grappling with this patchwork regulatory system since long before HIPAA's enactment.").

whether they are 'contrary' to the corresponding federal standard and, if so, whether they are 'more stringent.'"[106]

Thus, while this approach might allow states to enhance HIPAA protections, or fill in their gaps, it is not perfect. Without uniformity, these varied laws are very burdensome to both health care providers and patients.

2. *Torts*

Many writers have suggested using torts to enforce medical privacy.[107] One reason is that torts "allow plaintiffs who have been legitimately harmed by unauthorized medical records disclosure[s] to recover for their injur[ies]," while preventing frivolous and fake claims.[108] Torts were also the general way medical privacy was enforced pre-HIPAA.[109] Lastly, the threat from tort damages makes covered entities more likely to follow medical privacy standards because they understand "failure to do so may result in a multitude of large damages awards that are not subject to the HIPAA statutory cap."[110] However, like statutory approaches, tort-based approaches vary wildly in both their required elements and theories, and face their own preemption problems.[111]

a. *The Restatement-Based Privacy Torts*

The Second Restatement of Torts recognizes four types of privacy right violations: 1) "unreasonable intrusion upon the seclusion of another," 2) "appropriation of the other's name or likeness," 3) "unreasonable publicity given to the other's private life," and 4) "publicity that unreasonably places the other in a false light before the public."[112] In states using the Restatement torts, victims of medical privacy violations can usually sue only for an unreasonable

---

[106] *Id.* at 505 ("State law provisions that are more stringent will survive and reverse preempt the federal law, while those that are less stringent will be preempted."). For a fuller discussion of the complex processes covered entities must comply with when crossing state lines, see *id.* at 505–12.

[107] *See, e.g.*, Collins, *supra* note 33, at 224–32; Michael Frankel, Note, *Do Doctors Have a Constitutional Right To Violate Their Patients' Privacy?: Ohio's Physician Disclosure Tort and the First Amendment*, 46 VILL. L. REV. 141, 143 (2001); Rutherford, *supra* note 34, at 214 ("The threat of damages in tort suits should improve compliance by the various entities subject to HIPAA regulation.").

[108] Collins, *supra* note 33, at 225. A tort-based solution could allow patients suffering actual harm to recover, but not allow "opportunistic plaintiffs to enforce regulations that should be left to the HHS Secretary's discretion." *Id.* (noting this would help prevent "frivolous litigation").

[109] *See id.*

[110] Rutherford, *supra* note 34, at 214.

[111] *See infra* Part IV.B.2.a.

[112] RESTATEMENT (SECOND) OF TORTS § 652A(1)–(2) (AM. LAW INST. 1977).

intrusion upon seclusion or unreasonable publicity given to another's private life.[113]

Oklahoma has adopted the Restatement approach.[114] In a 2006 case, the Western District of Oklahoma looked at both "intrusion upon the seclusion of another and unreasonable publicity given to the other's private life."[115] In *Doe v. Brundage-Bone Concrete Pumping Inc.*, the plaintiff, a construction employee, received medical treatment and temporary disability due to injuries.[116] While on disability, his employer erroneously received a health insurance form from a hospital visit unrelated to the plaintiff's worker's compensation claim.[117] The hospital then showed the employer "several pages of billing records," containing two pages "clearly includ[ing] references to treatment for a back injury" and a reference to a "CT CHEST W/O STAT" test, which he took back to his office.[118] The hospital disclosed the records believing he was "authorized to obtain" them because he "provided the necessary personal information to gain access."[119] While the employer actually did not have a release from the plaintiff, the plaintiff's 2003 hospital release indicated his records could be disclosed to parties necessary for workers' compensation claims.[120]

A few months later, the plaintiff attempted to get his job back, and while jobs were available, he was not offered one.[121] His employer claimed this was "because Plaintiff had previously indicated that he did not like the physically demanding work" or operating a certain machine.[122] However, the plaintiff alleged that the billing records contained his HIV treatment records.[123] He sued the hospital for medical privacy violations, claiming the disclosure cost him his job.[124]

First, the court rejected the "unreasonable publicity" claim, which requires unreasonable publicity given to a private fact, because disclosing the

---

[113] *See, e.g.*, Doe v. Brundage-Bone Concrete Pumping, Inc., No. CIV-05-1287-C, 2006 U.S. Dist. LEXIS 100042, at *10 (W.D. Okla. Aug. 23, 2006).

[114] *See id.*

[115] *Id.*

[116] *Id.* at *1–2.

[117] *Id.*

[118] *Id.* at *2. Another employee also saw these records on the employer's desk. *Id.*

[119] *Brundage-Bone*, 2006 U.S. Dist. LEXIS 100042, at *3. The hospital's first answer claimed the employer "identified himself as Plaintiff and requested copies of billing records," but amended this to say the clerk believed he was authorized. *Id.*

[120] *Id.*

[121] *Id.* at *3–4.

[122] *Id.* at *4.

[123] *Id.* at *4–5 ("[But] Van Nest and other employees . . . claim that they did not know that Plaintiff was HIV+ until [the] lawsuit was filed."). Plaintiff, therefore, brought suit on the theory that he was not offered the job because of his HIV status. *See id.* at *4–6.

[124] *Id.* at *10.

information to a small number of coworkers was not publication.[125] Next, the court rejected the intrusion upon seclusion claim, which requires "nonconsensual intrusion" that is "highly offensive to a reasonable person."[126] Both the intrusion itself and the hospital employee's conduct in giving out the record to the employer, whom he believed was the plaintiff despite no affirmative misrepresentation of identity, were not highly offensive to a reasonable person.[127]

b. *The Cons of a Restatement Approach Outweigh the Benefits*

Brundage-Bone highlights the benefits and problems of applying traditional privacy tort theories to medical privacy violations. First, both tort theories beneficially eliminate the confidentiality problem in other tort theories like negligence and confidentiality breach. Using these torts can "eliminate the need for a confidential relationship and rely solely on the disclosure of confidential information."[128] As for the intrusion upon seclusion claim, it has the benefit of not requiring publication.[129] This is useful in medical privacy cases where the information was not disclosed to the general public, but "the disclosure itself [was] nonetheless extremely injurious."[130] However, there are problems here as well.

Even unintentional privacy violations that aren't highly offensive to most people can cause serious harms. A doctor leaving out a patient file or a government agency improperly disclosing private information may not be intentional, but the harms felt by victims are still real. Furthermore, the risk of suit for unintentional violations will deter future abuses and make actors more careful than they otherwise might be. For many of these same reasons, the "highly offensive" requirement might not always be satisfied in medical privacy cases. While many consider their medical information very sensitive and, as individual victims, would find an improper disclosure highly offensive,[131] it is

---

[125] *Brundage-Bone*, 2006 U.S. Dist. LEXIS 100042, at *10 (granting summary judgment for employer on the unreasonable publicity claim).

[126] *Id.* at *11 (granting summary judgment for employer on the intrusion-upon-seclusion claim).

[127] *Id.* at *11–12. The employer was wearing a shirt with his own name on it. *Id.* The court also noted the "issue of fact as to why [the employer] wanted those records and what he hoped to learn," but the evidence was still not strong enough to show highly offensive conduct. *Id.* at *12. The court, however, declined to base summary judgment on consensual intrusion because the employer may have acted "beyond the scope of the limited consent" provided by the 2003 release "in violation of Plaintiff's reasonable expectation of privacy." *Id.* at *12 n.4.

[128] *See* Oates, *supra* note 38, at 768.

[129] RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (AM. LAW INST. 1977).

[130] *See* Oates, *supra* note 38, at 764.

[131] *Id.* at 771; *see also* LYGEIA RICCIARDI, CONSUMER PARTNERSHIP FOR EHEALTH, PROTECTING SENSITIVE HEALTH INFORMATION IN THE CONTEXT OF HEALTH INFORMATION TECHNOLOGY 2 (June 2010), http://www.nationalpartnership.org/research-library/health-

possible a reasonable person would not find it offensive.[132] Imposing the reasonable person standard on something as important, complex, and contoured as medical privacy ignores the severe harm individuals can feel from privacy violations.

The "publicity given to private life" tort faces similar problems, as shown in *Brundage-Bone* where the plaintiff was denied recovery because the exposure of his medical records, including the potential release of his HIV+ status, to a group of coworkers was not publication.[133] The ruling did not speak to the underlying personhood and privacy harm, but rather to the number of people the information was disclosed to, thus leaving the plaintiff without remedy.[134] The Restatement clarifies that "publicity" "means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[135] This is unlikely in many medical privacy cases, so victims who experience painful and embarrassing disclosures only to small groups are left without remedy.[136]

In sum, while the general Restatement torts have definite benefits for individuals seeking to recover in medical privacy suits, their limits prevent them from adequately protecting victims of medical privacy violations. Outside of these traditional torts, some states also go further and incorporate HIPAA standards into their tort-remedy frameworks.

c. *HIPAA-Influenced Torts*

Many states also recognize traditional tort claims, such as negligence or breach of confidentiality, in the realm of medical privacy.[137] However, the new trend seems to be towards allowing HIPAA to influence these traditional torts.[138] Essentially, some courts have found that "to the extent it has become the common practice for [state] health care providers to follow the procedures required under HIPAA in rendering services to their patients, HIPAA and its

---

care/HIT/protecting-sensitive-health.pdf [https://perma.cc/Y34F-VBNK]. With sensitive medical information relating to things like domestic violence, abortion, substance abuse, STDs, etc., patients risk possible "discrimination, social stigma, and physical harm." *Id.* at 2–3. This information can sometimes extend beyond risks to the individual patient, and also affect families and employers. *See id.* at 2.

[132] *See* Collins, *supra* note 33, at 226.

[133] *See* Doe v. Brundage-Bone Concrete Pumping, Inc., No. CIV-05-1287-C, 2006 U.S. Dist. LEXIS 100042, at *10 (W.D. Okla. Aug. 23, 2006).

[134] *Id.* at *22.

[135] RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (AM. LAW INST. 1977).

[136] Collins, *supra* note 33, at 226–27; Oates, *supra* note 38, at 764.

[137] *See, e.g.*, Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 36 (Conn. 2014); R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 723–24 (W. Va. 2012).

[138] *See Byrne*, 102 A.3d at 42.

implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence."[139]

One of the most recent and well-publicized[140] cases comes from the Connecticut Supreme Court.[141] The plaintiff in *Byrne v. Avery Center for Obstetrics & Gynecology*, Emily, sued her obstetrics and gynecology (OBGYN) office after it released her private medical information, without her authorization, in response to a subpoena.[142] Emily specifically instructed the OBGYN not to release her information to Mendoza, her ex-boyfriend and father of her child, in 2004, but a Connecticut court subpoenaed the records after Mendoza filed a paternity suit against Emily in 2005.[143] Without ever notifying Emily about the subpoena or attempting to quash it, the OBGYN mailed her file to the court where Mendoza viewed it in the court file.[144] Emily was later able to seal her medical file, but claimed Mendoza harassed and threatened her after he initially viewed the records.[145]

Emily sued the OBGYN, alleging it "acted negligently by failing to use proper and reasonable care in protecting her medical file, including disclosing it without authorization in violation of [state laws] and the department's regulations implementing HIPAA."[146] The lower court found that all actions dealing with private medical information were preempted by HIPAA, and that because "HIPAA does not create a private right of action, . . . claims of violations instead [must] be raised through the department's administrative channels."[147] The lower court believed the plaintiff's negligence claims were actually just relabeled HIPAA claims.[148] In response, Emily said her claims were not HIPAA private action claims, but were instead for common-law negligence "with HIPAA informing the standard of care."[149]

---

[139] *Id.* at 49. Some courts have allowed plaintiffs to use HIPAA violations as a basis for state negligence per se claims. *See, e.g.*, Harmon v. Maury Cty., No. 1:05-0026, 2005 U.S. Dist. LEXIS 48094, at *8–11 (M.D. Tenn. Aug. 31, 2005); *St. Mary's Med. Ctr.*, 735 S.E.2d at 723.

[140] *See, e.g.*, Allison Grande, *HIPAA Doesn't Preempt Negligence Claims: Conn. High Court*, LAW360 (Nov. 6, 2014), https://www.law360.com/articles/594162/hipaa-doesn-t-preempt-negligence-claims-conn-high-court (on file with *Ohio State Law Journal*); Joseph J. Lazzarotti, *Negligence Claims for Breach of Patient Privacy Not Preempted by HIPAA, Connecticut Supreme Court Holds*, NAT'L L. REV. (Nov. 10, 2014), http://www.natlawreview.com/article/negligence-claims-breach-patient-privacy-not-preempted-hipaa-connecticut-supreme-cou [https://perma.cc/95S5-EGYR].

[141] *Byrne*, 102 A.3d at 32.

[142] *Id.* at 36. The OBGYN also notified her "that it would not disclose [her] health information without her authorization." *Id.*

[143] *Id.*; Grande, *supra* note 140.

[144] *Byrne*, 102 A.3d at 36.

[145] *Id.*

[146] *Id.* at 36–37 (footnote omitted) (listing other claims, including breach of contract, negligent misrepresentation, and negligent infliction of emotional distress).

[147] *Id.* at 37.

[148] *See id.* at 38.

[149] *Id.* at 41.

The Connecticut Supreme Court first agreed that HIPAA's statutory structure precludes a private cause of action for medical privacy violations.[150] However, it also noted that federal laws normally do not preempt state causes of action purely because they impose higher liabilities.[151] The court then concluded that HIPAA's regulatory history demonstrated it was not meant to "preempt tort actions under state law arising out of the unauthorized release of a plaintiff's medical records."[152] Lastly, based largely on precedents from other states, the court found that HIPAA could inform the standard of care for negligence claims "arising from allegations of negligence in the disclosure of patients' medical records pursuant to subpoena."[153] However, the court did not decide if Connecticut actually recognized "claims arising from a health care provider's alleged breach of its duty of confidentiality in the course of complying with a subpoena," so actual negligence would depend on the lower court's finding on remand.[154]

This finding has been hailed as "precedent-setting"[155] and "a reminder to [covered entities] . . . that failing to comply with HIPAA [can] result not only in government enforcement but also claims of negligence brought by individuals."[156] While this is an achievement for plaintiffs,[157] this holding arguably has many unaddressed problems.

i. *Preemption Problems*

The preemption problem here is twofold. First, rather than applying the case-by-case and law-by-law preemption analysis envisioned by HIPAA,[158] the court made a sweeping pronouncement without regard to settled law around HIPAA's applicability and preemption.[159] While it concluded that HIPAA-influenced torts were not preempted, that conclusion rests on an illusory basis

---

[150] *Byrne*, 102 A.3d at 43–45.

[151] *Id.* at 45.

[152] *Id.* at 46.

[153] *Id.* at 49.

[154] *See id.*

[155] Albeit in a statement from Emily's attorney. Grande, *supra* note 140.

[156] Douglas Dahl, *What Preemption? Connecticut State Court Gives Life to Negligence Claims Based on HIPAA Privacy Standard of Care*, PROSKAUER: PRIVACY L. BLOG (Dec. 22, 2014), http://privacylaw.proskauer.com/2014/12/articles/hipaa-1/what-preemption-connecticut-state-court-gives-life-to-negligence-claims-based-on-hipaa-privacy-standard-of-care/ [https://perma.cc/E7VN-4JHC].

[157] *See* Rutherford, *supra* note 34, at 211.

[158] *See Preemption of State Law*, *supra* note 90 ("Since preemption is a judicially developed doctrine, it is reasonable to interpret this term as indicating that the statutory analysis should tie in to the analytical formulations employed by the courts. Also, [these] court-developed tests . . . represent a long-term, thoughtful consideration of the problem of defining when a state/federal conflict exists. They will also, we assume, generally be employed by the courts when conflict issues arise . . . .").

[159] *See Byrne*, 102 A.3d at 49.

since the court did not analyze if the tort was actually recognized in Connecticut.[160] In other words, the court did a preemption analysis on a state tort that did not actually exist.[161]

The second, and larger, problem is that HIPAA-influenced torts are essentially attempts to dress up HIPAA claims and avoid the fact that HIPAA does not create a private right of action.[162] Only Congress can create a "private right[] of action to enforce federal law," and when these issues come up, courts should "interpret the statute Congress has passed to determine whether it displays an intent to create not just a private right but also a private remedy."[163] Unless both exist, then courts cannot create a private right of action, even if such an option would be desirable as a policy matter or "compatible with the statute."[164]

Courts addressing HIPAA issues have consistently found no private right of action and that Congress showed no intent to create a private right or remedy.[165] Instead, Congress required that the "Secretary" comply with the statute,[166] that "[t]he Secretary . . . establish specifications for implementing each of the standards adopted under this part,"[167] and that the Secretary impose fines and punishments for violations of the Act.[168] Even when promulgating regulations, the HHS noted that it did not "have the legislative authority to grant a private right of action to sue under this statute" for privacy breaches, and "[o]nly Congress [could] grant that right."[169] Thus, there is no way to infer a private cause of action from HIPAA itself.

---

[160] *See id.* at 49.

[161] *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., No. FBTCV076001633S, 2015 WL 5236816, at *5–7 (Conn. Super. Ct. Aug. 3, 2015) (refusing to recognize a "common-law duty of confidentiality," despite the Connecticut Supreme Court's assumption that the common law recognized such an action).

[162] *See* Brief of the Defendant-Appellee at 10–14, *Byrne*, 102 A.3d 32 (No. 18904). As an Ohio court recently noted when declining to recognize a HIPAA-influenced tort, "to the extent that HIPAA universally has been held not to authorize a private right to action, to permit HIPAA regulations to define per se the duty and liability for breach is no less than a private action to enforce HIPAA." Sheldon v. Kettering Health Network, 40 N.E.3d 661, 674 (Ohio Ct. App. 2015); *see also* Skinner v. Tel-Drug, Inc., No. CV-16-00236-TUC-JGZ (BGM), 2017 U.S. Dist. LEXIS 12427, at *8–10 (D. Ariz. Jan. 27, 2017) (rejecting a negligence per se claim based on HIPAA establishing the duty of care, in part because HIPAA lacks a private right of action and enforcing it via negligence per se is the same as enforcing it via private action).

[163] Alexander v. Sandoval, 532 U.S. 275, 286 (2001).

[164] *Id.* at 286–87. In *Sandoval*, the Court refused to create a private right of action "to enforce disparate-impact regulations promulgated under Title VI of the Civil Rights Act of 1964." *Id.* at 278, 293.

[165] *See supra* note 62 and accompanying text; *infra* notes 220–25 and accompanying text.

[166] *See* 42 U.S.C. § 1320d-1(f) (2012).

[167] *Id.* § 1320d-1(d).

[168] *Id.* § 1320d-5(a)(1).

[169] Standards for Privacy, *supra* note 46, at 82,566.

Furthermore, HIPAA does not preempt state laws relating "to the privacy of individually identifiable health information" that are "more stringent" than the Privacy Rule.[170] However, courts using HIPAA-influenced negligence claims seemingly fail to recognize that the federal statute defines a state law that "[r]elates to the privacy of individually identifiable health information" as one that either has the "specific purpose of protecting the privacy of health information" or that "affects the privacy of health information in a direct, clear, and substantial way."[171] These state torts may be more stringent than HIPAA, but it is not clear that they actually affect the privacy of health information directly, clearly, or substantially, and they certainly lack the specific purpose of protecting the privacy of health information.[172] They only affect medical privacy clearly once the HIPAA standards are applied.[173] This leads to serious questions about whether or not these claims are actually preempted, which is another avenue toward the problem of varied interpretations between states and unclear doctrine.

ii. *Other Problems with HIPAA-Influenced Torts*

Outside of the preemption issues with HIPAA-influenced torts, other problems exist as well. First, many of these torts focus on the confidential relationship between doctor and patient.[174] While this is sometimes beneficial,[175] it ignores situations where the person wrongfully disclosing the information is not a health care worker. As HHS notes on its website, "[m]any organizations that have health information about [individuals] do not have to follow" HIPAA's regulations.[176] Such organizations include life insurers, "[m]any state agencies like child protective service agencies," and "[m]ost schools."[177] These entities also lack the confidential patient–doctor relationship in HIPAA-influenced tort cases.[178]

---

[170] 45 C.F.R. § 160.202 (2016).

[171] *Id.* § 160.203(b).

[172] *See* Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999) (noting that traditional tort theories such as "invasion of privacy, defamation, implied breach of contract, . . . negligence, and medical malpractice" are "ill-suited" for medical privacy claims because they are designed to protect other interests and "only coincidentally overlap that of preserving patient confidentiality").

[173] *See, e.g.*, Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 35 (Conn. 2014).

[174] *See* Collins, *supra* note 33, at 227. For example, the HIPAA-influenced tort in *Byrne* grew from "a health care provider's breach of its duty of confidentiality." *Byrne*, 102 A.3d at 36.

[175] *See* Collins, *supra* note 33, at 227–28 (noting these claims do not rely on intent, offensiveness, or publicity).

[176] HHS, *Your Rights Under HIPAA*, *supra* note 54.

[177] *Id.*

[178] While these are problems in HIPAA-based tort cases, they would also be applicable in non-HIPAA-based tort cases based on negligence or breach of confidentiality.

Second, there remains the serious possibility of creating disparities within HIPAA itself by having various state interpretations of federal rules rather than leaving it up to the federal agency. As state courts determine how much HIPAA has influenced their standard of care, or what it means to be "more stringent" than the federal rule, they are creating varying interpretations that are bound to differ between the states.[179] Thus, although these torts help plaintiffs recover, they create ambiguity and destroy uniformity among the states. They also create a questionable preemption analysis that will likely cause more litigation as courts have to figure out how to apply a complex federal law.

V. FIXING THE MESS: HOW NON-HIPAA-INFLUENCED TORTS AND SUPREME COURT GUIDANCE CAN HELP SOLVE THESE PROBLEMS

In light of the previous principles and various, confusing solutions, this Note first suggests that courts should adopt a non-HIPAA-based tort approach, similar to that taken in Ohio. While this is by no means the majority approach so far, it avoids more potential preemption problems and allows more state-based control in this important area of litigation. Furthermore, this approach allows for victim compensation, unlike HIPAA itself. One of HIPAA's largest problems is its lack of victim compensation, which could serve to deter future violations and to make victims whole again.[180] While Congress and HHS obviously recognized that "[p]rivacy is a fundamental right," victims have fallen by the wayside.[181]

Second, regardless of which approach the states choose, this Note asserts that the U.S. Supreme Court needs to take a preemption case and rule on this issue because the now heavily varied state standards create a patchwork of confusing legal rules, and individuals' important privacy rights should not vary based on which state they live in.[182] While this Note advocates for the Court to find that HIPAA-based torts are preempted because they are essentially dressed-up HIPAA claims contrary to the regulatory scheme and are not more stringent than current protections, any clarification of HIPAA preemption issues would be generally welcomed.

---

[179] *See infra* notes 241–45 and accompanying text.

[180] HIPAA's enforcement focus is on "education, technical assistance, and voluntary compliance[,] and not on finding violations and imposing penalties." Standards for Privacy, *supra* note 46, at 82,604.

[181] *See id.* at 82,464. While much of the public and governmental attention focuses on security breaches for larger groups of people, "it's often little-noticed smaller-scale violations of medical privacy—the ones that affect only one or two people—that inflict the most harm." Ornstein, *Small-Scale Violations*, *supra* note 36.

[182] *See, e.g.*, *In re* Cmty. Health Sys., Inc., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *87–94 (N.D. Ala. Sept. 12, 2016) (dismissing some, but not all, HIPAA-based negligence per se claims against defendants based on differing state laws surrounding "whether a plaintiff may pursue a negligence *per se* claim based on an alleged violation of a federal statute that does not provide a private right of action").

A. *Ohio's Medical Privacy Tort: An (Imperfect) Independent Tort Model*

In contrast to the HIPAA-influenced torts, Ohio uses an independent, non-HIPAA-based tort approach.[183] The evolution of Ohio's "independent tort . . . for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship" has evolved over time.[184] As early as 1965, Ohio recognized a tort for "[t]he unauthorized revelation of medical secrets, or *any* confidential communication given in the course of treatment."[185] This was premised on the idea of an implied contract in the doctor–patient relationship "that any confidential information gained through the relationship will not be released without the patient's permission."[186]

In 1999 (prior to the Privacy Rule), the Ohio Supreme Court affirmed this tort's existence, but clarified it as "an independent common-law tort of breach of confidence in the physician-patient setting."[187] This was not an absolute privilege, and it did allow for medical providers to disclose when required by statutory or "common-law duty, or where disclosure [was] necessary to protect or further a countervailing interest which outweigh[ed] the patient's interest in confidentiality."[188] As for the "authorization" requirement, consents "to release medical information [had to] be fairly specific in terms of to whom the release [was] made."[189]

In a post-HIPAA world, Ohio courts began reexamining this tort more closely and have struggled with where exactly HIPAA fits in.[190] In 2012, Ohio's Tenth Appellate District addressed whether this tort still existed in *OhioHealth Corp. v. Ryan*.[191] There, the court granted dismissal for OhioHealth Corporation for allegedly creating "false identifiable health information" about the appellant and disclosing it to a third party for payment purposes.[192]

The court held that "[e]ven if we assume that *Biddle* allows a claim for an independent tort against a health care provider for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information learned via a physician-patient relationship," when the information involves

---

[183] This Note endorses a non-HIPAA-based tort approach, though not exactly in the same way as it has been construed in Ohio. *See infra* Part V.B.

[184] Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999).

[185] Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 802 (N.D. Ohio 1965).

[186] *Id.* at 801.

[187] *Biddle*, 715 N.E.2d at 522.

[188] *Id.* at 524 (e.g., public safety concerns).

[189] *Id.* at 527.

[190] *See, e.g.*, OhioHealth Corp. v. Ryan, No. 10AP-937, 2012 WL 68733, at *3–5 (Ohio Ct. App. Jan. 10, 2012).

[191] *See id.*

[192] *Id.* at *1.

account information, the claim would fail.[193] This was because the release of information for payment was authorized under HIPAA (meaning it was not unauthorized), and because the tort was preempted by HIPAA.[194] Thus, the court said that HIPAA both informed the tort's authorization requirement and preempted the tort. This was a confusing standard that could presumably be solved by finding "authorization" is independent from HIPAA, which is what Ohio's Second Appellate District did in 2015 in *Sheldon v. Kettering Health Network*.[195]

In *Sheldon*, the court tried to answer "whether *Biddle*['s] common-law right of action recognized in 1999 survive[d] HIPAA."[196] The plaintiffs asserted that the defendant's medical information storage system normally prevented unauthorized access per HIPAA requirements, but an administrator, Sheldon, had unauthorized access to the plaintiffs' medical records.[197] He "improperly accessed extremely sensitive medical information" about his ex-wife and shared it.[198] There were also other "significant" breach incidents, which could have been prevented if the health network had reasonably run reports and monitored the system.[199] The plaintiffs sued for "common-law tort claims for invasion of privacy, negligence, negligence per se, negligent training, negligent supervision, intentional infliction of emotional distress, and breach of fiduciary duty."[200]

First, the court noted that the individual torts against Sheldon did not "necessarily appear to depend on an alleged HIPAA violation," and that the common-law claims against him for "improperly accessing and sharing the plaintiffs' health information" could be brought regardless of HIPAA.[201] However, the court refused to hold Kettering Health Network vicariously liable for this behavior, as it was outside the scope of his employment.[202]

Next, the court concluded that HIPAA did not preempt the *Biddle* torts against the hospital for "invasion of privacy, negligence, negligence per se, negligent training, negligent supervision, intentional infliction of emotional

---

193 *Id.* at *4.

194 *Id.*

195 *See* Sheldon v. Kettering Health Network, 40 N.E.3d 661, 671 (Ohio Ct. App. 2015).

196 *Id.*

197 *Id.* at 665–67.

198 *Id.* at 666.

199 *Id.*

200 *Id.* at 664. An important issue on appeal was whether the health network was vicariously liable for Sheldon's actions. *Id.* at 667. However, the plaintiff also asserted that governmental HIPAA enforcement did not "preclude[] a private individual from bringing a tort action" and that "[c]ommon sense and public policy . . . support[] that common law causes of action should be permitted even where they overlap with HIPAA violations." Plaintiff-Appellant's Brief at 9, *Sheldon*, 40 N.E.3d 661 (No. 26432).

201 *Sheldon*, 40 N.E.3d at 667.

202 *Id.* at 668–69.

distress, and breach of fiduciary duty."[203] The court found no evidence that the tort actually conflicted with HIPAA because the claim did not assert "recovery for release of information that HIPAA specifically allows."[204] Allowing individual damage recovery did not interfere with federal enforcement, meaning providers could comply with both rules, and allowing such damages could enhance patient protections.[205] The "independent tort recognized in *Biddle* [was] still viable after HIPAA[,] although the parameters of such a claim may have been impacted by HIPAA preemption."[206] The court noted the "conundrum" about the "unauthorized" requirement, finding that disputes about valid authorizations would likely lead to HIPAA references.[207] Using HIPAA to determine authorization might allow for HIPAA enforcement via state tort, "which is arguably contrary to the overwhelming conclusion that HIPAA does not provide a private right of action."[208] Because "authorization" was not the question in this case, the court did not resolve the problem.[209]

However, the court refused to accept HIPAA as the standard of care for negligence claims or the basis for negligence per se, as this would be "tantamount to authorizing a prohibited private right of action for violation of HIPAA itself."[210] Regarding the "HIPAA-based" claim for breach of confidentiality, the court did not address HIPAA's impact on the tort, but rather concluded that there was not sufficient disclosure for the *Biddle* tort to apply.[211]

While the Ohio court did not answer the question of how HIPAA impacts "authorization" in its tort, it did recognize that the tort can exist independently of HIPAA. Thus, it avoids the preemption problem of the HIPAA-based torts, which essentially create a disguised private right of action. Furthermore, allowing heightened recovery does not interfere with federal enforcement

---

[203] *Id.* at 670–72. The plaintiffs claimed their suit was not based on HIPAA, but the court believed the complaint was "grounded in the notion that KHN's actions were wrongful *because* they failed to take steps[] consistent with HIPAA." *Id.* at 670. Nevertheless, the court interpreted "the complaint broadly to determine whether the allegations assert[ed] common-law tort claims independent from HIPAA." *Id.*

[204] *Id.* at 672.

[205] *Id.* Thus, the tort still exists in Ohio. *Id.* However, the court did not clarify whether this tort is limited to *intentional* disclosures. *See id.* at 672–73. The court could not find sufficient evidence that the health network "actively or intentionally disclosed anything." *Id.* at 673. The *Biddle* tort "itself dealt with deliberate intentional disclosure," which would survive a motion to dismiss either "pre- or post-HIPAA, with or without reference to HIPAA regulations." *Id.*

[206] *Id.* at 673.

[207] *Sheldon*, 40 N.E.3d at 673.

[208] *Id.*

[209] *Id.*

[210] *Id.* at 672, 674 ("[T]o permit HIPAA regulations to define per se the duty and liability for breach is no less than a private action to enforce HIPAA, which is precluded."). The court also rejected HIPAA as a standard based on Ohio precedent that a violation of administrative rules is not grounds for negligence per se, and because HIPAA does not actually create standards "for when and how information security audits should be performed." *Id.* at 674.

[211] *Id.* at 674–75.

efforts, which as stated previously are lax anyway,[212] but can actually enhance the protection of individually identifiable health information.

B. *An Independent Tort Is the Best Approach*

An independent, non-HIPAA-based tort approach avoids many of the problems with HIPAA-based approaches.[213] This is not to say that the other approaches are necessarily preempted by HIPAA, but rather that this approach creates fewer potential problems, and on its face appears to be more closely aligned to HIPAA's goals, purposes, and language.[214]

It is undisputed that HIPAA does not create a private right of action,[215] meaning one cannot sue an individual, hospital, doctor, or other entity when their HIPAA rights are violated. In fact, HHS commentary for the Privacy Rule notes that HHS does "not have the authority to provide a right of action by regulation."[216] However, allowing for HIPAA-based torts, in effect, creates a semiprivate right of action under HIPAA, going against HIPAA's enforcement scheme.[217] Furthermore, because these claims have a higher likelihood of succeeding than actual HIPAA claims,[218] it is foreseeable that plaintiffs will be

---

[212] *See supra* Part III.B.

[213] For a discussion of HIPAA-based torts and their problems, see *supra* Part IV.B.2.

[214] Because all state torts require slightly different elements, it is almost impossible to say which are actually preempted. However, this Note advocates for the path with the fewest preemption problems.

[215] Dodd v. Jones, 623 F.3d 563, 569 (8th Cir. 2010); Acara v. Banks, 470 F.3d 569, 571–72 (5th Cir. 2006) (per curiam); Runkle v. Gonzales, 391 F. Supp. 2d 210, 237 (D.D.C. 2005); Swift v. Lake Park High Sch. Dist. 108, No. 03 C 5003, 2003 U.S. Dist. LEXIS 18684, at *9 (N.D. Ill. Oct. 21, 2003) ("No federal court reviewing the matter has ever found that Congress intended HIPAA to create a private right of action."); Agee v. United States, 72 Fed. Cl. 284, 289–90 (Fed. Cl. 2006); Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 45 (Conn. 2014); *Sheldon*, 40 N.E.3d at 670.

[216] Standards for Privacy, *supra* note 46, at 82,605. This is not to say that HHS does not believe there should be a private right under HIPAA. In fact, in testimony before the Senate Committee on Labor and Human Resources regarding HIPAA, HHS Secretary Shalala in 1998 said that in order to "give redress to the victims[,] . . . individual[s] whose rights under the federal privacy law have been violated . . . should be permitted to bring a legal action for actual damages and equitable relief." Donna E. Shalala, *Testimony of Secretary of Health and Human Services, September 11, 1997*, U.S. DEP'T HEALTH & HUM. SERVS. (Feb. 1, 1998), https://aspe.hhs.gov/testimony-secretary-health-and-human-services-september-11-1997 [https://perma.cc/4MTK-QDEB].

[217] *See Sheldon*, 40 N.E.3d at 673 (explaining the semi-private right of action under *Biddle*); *see also* Poore-Rando v. United States, No. C16-5094 BHS, 2017 U.S. Dist. LEXIS 145085, at *14 (W.D. Wash. Sept. 7, 2017) ("[The] vague reliance on the HIPAA 'privacy rule' . . . cannot be used to establish a per se intrusion or reasonable expectation of privacy . . . [because] 'to permit HIPAA regulations to define per se the duty and liability for breach is no less than a private action to enforce HIPAA, which is precluded.'" (quoting Skinner v. Tel-Drug, Inc., No. CV-16-00236-TUC-JGZ (BGM), 2017 U.S. Dist. LEXIS 12427, at *9 (D. Ariz. Jan. 27, 2017))); *supra* notes 62, 166–73 and accompanying text.

[218] *See supra* Part III.B (regarding lack of enforcement).

more likely to bring them than actual HIPAA claims. Congress and HHS created a complex scheme meant to deter violations, educate providers, and protect individuals,[219] but this will be undermined if medical privacy victims largely choose HIPAA-influenced state torts over HIPAA itself.

Creating such a private right of action is not a practical idea and is not what Congress intended.[220] In *Acara v. Banks*, the Fifth Circuit noted that since HIPAA lacked an express private right, it had to "determine if such [a right was] implied within the statute."[221] HIPAA lacked "express language conferring privacy rights upon a specific class of individuals," but instead focused on regulating those who access private medical information and conduct "electronic health care transactions."[222] It also provided for "both civil and criminal penalties," with enforcement limited to the HHS Secretary.[223] This delegation of enforcement power was a "strong indication that Congress intended to preclude private enforcement."[224] After noting that every district court nationwide that had addressed the issue had also found "Congress did not intend for private" HIPAA enforcement, the circuit court found that HIPAA lacked a private cause of action.[225]

There is also "uncertainty as to whether judges and juries are best equipped to determine if a violation has even occurred."[226] HIPAA's Privacy Rule is a complex regulation, and while some of its provisions are straightforward, many are not.[227] For example, while HIPAA's regulations lay out the definition for "more stringent" laws in 45 C.F.R. § 160.202, courts have been inconsistent in applying this definition.[228] In *West Virginia Department of Health & Human Resources v. E.H.*, the West Virginia Supreme Court of Appeals simply stated that since the state's Department of Health and Human Resources determined its own regulations were more stringent than the federal requirements, they were not preempted by HIPAA.[229] As the dissent in that case points out, "This total lack of analysis makes no sense. . . . Surely Congress did not mean for HIPAA and the Supremacy Clause to be defeated in such a self-serving manner."[230]

This problem is also evident in the current leading case using HIPAA as the standard of care. In *Byrne*, the Connecticut Supreme Court held that "to the

---

[219] *See supra* Parts II.B, II.C.

[220] *See* Standards for Privacy, *supra* note 46, at 82,566 (stating that only Congress has authority to create a private cause of action); *see also Acara*, 470 F.3d at 570–72.

[221] *Acara*, 470 F.3d at 571.

[222] *Id.*

[223] *Id.*

[224] *Id.*

[225] *Id.* at 571–72. No other circuit courts besides the Fifth Circuit have considered the issue of whether Congress intended to create a private right of action for HIPAA. *Id.* at 571.

[226] Brill, *supra* note 62, at 2131.

[227] *See id.*

[228] *See* W. Va. Dep't of Health & Human Res. v. E.H., 778 S.E.2d 728, 744 (W. Va. 2015) (Davis, J., dissenting).

[229] *Id.* at 739–40 (majority opinion).

[230] *Id.* at 744 (Davis, J., dissenting); *see also* Standards 2002, *supra* note 47, at 53,266.

extent [HIPAA] has become the common practice for Connecticut health care providers to follow . . . in rendering services to their patients, [it] may be utilized to inform the standard of care" for negligence claims regarding "disclosure of patients' medical records pursuant to a subpoena."[231] Because HIPAA is a highly technical regulation, it may be difficult for courts to determine to what extent it has informed the standard of care and what the violation specifically is. In *Byrne*, the plaintiff's negligence claim was that the covered entity "acted negligently by failing to use proper and reasonable care in protecting her medical file, including disclosing it without authorization in violation of" state law claims and HIPAA.[232] This necessarily required the state judge to determine whether or not there was a HIPAA violation, rather than the federal agency who designed the regulations.

While it is not impossible for judges to determine when a HIPAA violation has occurred, it seems contrary to HIPAA's purpose to allow this type of variation among the states. In the purposes section of the Privacy Rule's initial promulgation, HHS stressed the importance of the "[n]eed for a [n]ational [h]ealth [p]rivacy [f]ramework" because "[p]rivacy is a fundamental right."[233] With individual judges and individual states determining what constitute HIPAA violations rather than HHS, this national framework is undermined.

Also, it is logical to conclude that HHS did not intend for HIPAA to create the standard of care in state actions. In the implementation regulations, HHS noted it did not "intend this regulation to describe a set of . . . 'best practices,'" but rather "a set of basic consumer protections and a series of regulatory permissions for use and disclosure of health information."[234] While the regulations are the "mandatory floor," HHS expected "covered entities to rely on their professional ethics and use their own best judgments in deciding which of these permissions they [would] use."[235] In describing the enforcement section, HHS also noted that "civil monetary penalties and . . . referrals for criminal prosecution," were only to be used when "voluntary compliance [could not] be achieved."[236] This cuts against allowing damages recovery for violations as determined by state courts, which may not take into account HHS's goal of achieving HIPAA compliance without the immediate use of penalties.[237]

---

[231] Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 49 (Conn. 2014).

[232] *Id.* at 36.

[233] Standards for Privacy, *supra* note 46, at 82,464.

[234] *Id.* at 82,471.

[235] *Id.*

[236] *Id.* at 82,472.

[237] Allowing HIPAA to be the standard of care is the same as enforcing HIPAA through a private right of action. It allows individuals to sue for HIPAA violations against the clear intent of the statute. *See supra* notes 62, 166–69 and accompanying text. The approach advocated in this Note avoids this dilemma by separating HIPAA from the private cause of action. This way, one cannot sue for HIPAA violations specifically, but can still receive vindication and compensation for the harms done to them by medical information disclosures.

C. *Ohio's Independent Tort Approach Provides a Base Model for Other Independent Tort Approaches*

The independent tort approach taken by Ohio seems to best avoid these problems.[238] Unlike HIPAA-based torts, an independent tort avoids facial preemption problems. Rather than creating a semiprivate right of action by allowing recovery when HIPAA has been violated, an independent tort can exist without reference to HIPAA standards.[239] Thus, judges and juries applying and analyzing this tort can refrain from analyzing complex, individual HIPAA requirements.[240] Instead, states can develop their own judicially crafted plans to protect their own citizens.

This approach also avoids the concerns about HIPAA variations among states resulting from HIPAA-influenced torts.[241] Rather than each state court system ruling on what constitutes HIPAA violations, with independent torts the states can continue their common-law protections that existed prior to HIPAA and develop their own independent systems that can be more stringent than HIPAA's requirements.[242] This avoids disrupting the national framework constituting what the federal government considers to be HIPAA violations.

However, the Ohio approach is not perfect. As noted above, there is a serious question regarding exactly what "unauthorized"[243] means in the Ohio *Biddle* tort.[244] While Ohio has not definitively ruled on whether HIPAA matters for purposes of authorization, a potential solution here is for the tort to go above and beyond HIPAA authorization in order to avoid preemption problems.[245] If, with regard to use or disclosure, the word "unauthorized" allows the state to "restrict[] a use or disclosure"[246] that would be permitted under HIPAA, or, with

---

[238] Although, as noted in Part V.B, this approach is currently not entirely consistent statewide and the courts have not fully set out the new parameters of the independent tort in a post-HIPAA world.

[239] *See* Sheldon v. Kettering Health Network, 40 N.E.3d 661, 672 (Ohio Ct. App. 2015).

[240] Even under this approach, however, there may be at least a cursory analysis of HIPAA. For instance, the independent tort claim in *Sheldon* was "not preempted because [the court] fail[ed] to see how such a claim [would] conflict[] with HIPAA unless the alleged claim assert[ed] recovery for release of information that HIPAA specifically allows." *Id.*

[241] There will still be variations among states in exactly how they formulate their tort approaches (precise method of recovery), but this will prevent inconsistent interpretations of HIPAA, a federal statute, which influences an individual's capacity to recover.

[242] Ohio courts have not analyzed if the independent tort is more stringent than HIPAA or not. The reasoning behind this is unclear, but one possible reason is that the tort requires an "active[] or intentional[]" element meaning. *Sheldon*, 40 N.E.3d at 673 ("Under any set of circumstances, pre- or post-HIPAA, with or without reference to HIPAA regulations, the intentional, unauthorized disclosures in *Biddle* should be actionable. Accordingly, we conclude that the independent tort recognized in *Biddle* is still viable after HIPAA although the parameters of such a claim may have been impacted by HIPAA preemption.").

[243] Does it mean unauthorized by HIPAA or by the person receiving medical care?

[244] *See supra* notes 205–09 and accompanying text.

[245] *See* 45 C.F.R. § 160.202 (2016) (defining "more stringent").

[246] *Id.*

regard to "the privacy of individually identifiable health information,"[247] allows the state to set standards that are "more stringent" than the HIPAA standards, then this would likely avoid preemption problems. The Ohio Supreme Court did not accept an appeal in *Sheldon v. Kettering Health Network*,[248] so the question of what it means to be "unauthorized" still remains.

D. *Improving the Independent Tort Approach: Moving Away from Preemption and Practical Problems*

There are many ways courts could improve upon Ohio's independent tort approach, both to safeguard against preemption problems and to avoid practical problems. First, to ensure that the tort's requirements are actually more stringent than HIPAA's Privacy Rule, courts could attach a high level of damages, including punitive damages, for violations. In implementing the Privacy Rule, HHS noted that HIPAA's penalties ("fines and imprisonment") "could be imposed in addition to the same type of penalty imposed by a state law."[249] HHS also stated that state laws allowing for individual recovery would not actually conflict with HIPAA's penalties.[250] In addition to there being no conflict, adding harsher penalties for medical privacy violations might make independent torts more stringent than current protections, which do not personally compensate victims. In response to a question about punitive damages, as well as other types of additional damages, HHS said it lacked the authority to promulgate such a damages rule, but that it believed "federal law should allow any individual whose rights have been violated to bring an action for actual damages and equitable relief."[251] It did not specifically reject the idea of punitive damages, so this would not necessarily be contrary to HIPAA.

As HHS notes on its website, state laws are "'more stringent' than the HIPAA Privacy Rule if [they] relate[] to the privacy of individually identifiable health information and provide[] greater privacy protections for individuals' identifiable health information."[252] In updating the independent tort approach for the modern era, state courts could expand the category of individuals that can be liable for medical privacy violations, which would seemingly provide greater privacy protections. Texas takes this approach through their statutory scheme,[253] and courts could adapt this to the common law by allowing more

---

[247] *See id.* § 160.203(b).

[248] Sheldon v. Kettering Health Network, 45 N.E.3d 244 (Ohio 2015) (mem.).

[249] Standards for Privacy, *supra* note 46, at 82,582.

[250] *Id.*

[251] *Id.* at 82,605.

[252] *See* HHS, *More Stringent*, *supra* note 88.

[253] *See* Hall & Nickel, *supra* note 99. Courts could also adopt some of the other Texas statutory provisions within their common law torts as well. For example, Texas provides for increased civil penalties "in addition to any penalties for violating federal laws." *Id.* It also requires covered entities to "provide patients with electronic copies of their electronic health records within 15 business days of the patient's written request," whereas HIPAA has a

entities to face liability for improper disclosures. In general, Ohio has not yet adopted a more expansive category of those potentially liable for unauthorized disclosures, limiting it instead to "a physician or hospital that commits an unauthorized and unprivileged disclosure and a third-party that induces the disclosure to be made."[254]

Another way to ensure independent torts are truly more stringent than the Privacy Rule's requirements is to expand the definition of "unauthorized disclosure." As mentioned previously, Ohio courts have been unclear about what "unauthorized" means in Ohio's independent tort, especially with regard to HIPAA regulations themselves.[255] At least one Ohio appellate court decision seems to cast doubt on whether the tort, as applied, is truly more stringent than HIPAA's requirements. In *Scott v. Ohio Department of Rehabilitation & Correction*, Ohio's Tenth District held that allowing "supervised [prison] inmate[s] access to trash containing unshredded medical documents" with other inmates' HIV status was not a "disclosure" under the tort, even when inmates then distributed that information to the general population, meaning that "unauthorized" disclosures could include unintentional actions . . . just not in this case.[256] This appears less stringent than HHS's given enforcement examples.[257] So, by expanding the definition of "unauthorized disclosures" to

---

thirty-day rule. *Id.* While it may be difficult to craft the specific deadline requirements into judicial solutions, courts could use them to influence damages (for example, the longer it takes to receive records equates to higher damages because it looks unreasonable). HHS even gives the example of state laws "that provide[] individuals with a right to inspect and obtain a copy of their medical records in a more timely manner than the Privacy Rule [as] 'more stringent.'" HHS, *More Stringent*, *supra* note 88. While this seems focused on the more statutory-based approach, there is no reason it could not extend to the common law.

[254] Templeton v. Fred W. Albrecht Grocery Co., 72 N.E.3d 699, 702 (Ohio Ct. App. 2017) (refusing to apply the independent tort to a plaintiff's employer after another employee accidently emailed his confidential psychological report to other employees). *But see* Hageman v. Sw. Gen. Health Ctr., 893 N.E.2d 153, 154 (Ohio 2008) ("[A]n attorney may be liable for the unauthorized disclosure to a third party of medical information regarding an opposing party that was obtained through litigation.").

[255] *See supra* notes 243–48 and accompanying text.

[256] Scott v. Ohio Dep't of Rehab. & Corr., 999 N.E.2d 231, 234, 240 (Ohio Ct. App. 2013). The court also found that the prison's decision not to have a "comprehensive medical trash disposal policy" was protected by discretionary immunity, meaning the prison could not be held liable for the tort. *Id.* at 238–39.

[257] For example, HHS's website details an enforcement action requiring a doctor's office to revise its fax cover page in addition to office-wide training on proper faxing procedures after the office mistakenly faxed a patient's medical records, which contained his HIV status, to his employer instead of his new provider. *See* HHS, *All Case Examples*, *supra* note 77. In another example, HHS detailed requiring a medical practice to reposition computer monitors, add privacy screens, and develop other safeguards after it displayed patient information to others on easily visible computer screens. *See id.* Leaving medical records in a place accessible by inmates is at least as improper and irresponsible as sending a mistaken fax and displaying private patient information on publicly visible screens, making Ohio's approach appear less stringent than Privacy Rule requirements.

include acts like leaving medical records in accessible trash, courts could help ensure the stringency of independent torts.

A practical problem victims of unauthorized disclosure face, especially in Ohio, is a lack of vicarious liability. While Ohio has not outright rejected vicarious liability, the *Sheldon* case is instructive with regard to the uphill battle victims face. In *Sheldon*, the court refused to recognize respondeat superior liability for the employer after the employee improperly accessed and shared the victim's health information.[258] Under Ohio law, the employee's unauthorized and improper actions were not done with the purpose of serving his employer, meaning they were not done within the scope of his employment.[259] Thus, the tort claims against the employer were dismissed. [260]

Indiana has taken the opposite approach, which should be instructive to courts implementing independent tort approaches. In *Walgreen Co. v. Hinchy*, an Indiana appellate court held Walgreen liable after one of its pharmacists (by the name of Withers) looked up the prescription record of her romantic partner's former significant other and gave it to her romantic partner.[261] The court stated that "the fact that a tortfeasor is empowered to commit the tort because of his employment weighs in favor of respondeat superior" liability before holding that since "some of Withers's actions were authorized," a jury consideration on the employer's liability was appropriate.[262] The court then affirmed the jury verdict finding Walgreen liable under respondeat superior for Withers's "tort of negligence by virtue of professional malpractice of a pharmacist."[263]

While the Indiana case was not an independent tort case, as advocated by this Note, the finding of respondeat superior liability is still instructive. The jury in *Hinchy* awarded the victim $1.8 million in damages, with both Walgreen and Withers jointly responsible for 80%.[264] It is unlikely that Withers as an individual could pay this entire amount, even though the jury found it reasonable for such a breach of medical privacy. In independent tort cases where the harm is essentially the same as in *Hinchy*, juries could award similar amounts that employee defendants are also unlikely to satisfy. However, if courts are willing to impose respondeat superior liability for employees' breaches of medical

---

[258] Sheldon v. Kettering Health Network, 40 N.E.3d 661, 668 (Ohio Ct. App. 2015).

[259] *Id.* at 669.

[260] *Id.* at 668.

[261] Walgreen Co. v. Hinchy, 21 N.E.3d 99, 104, 109–10 (Ind. Ct. App. 2014). The pharmacist, Withers, started dating her significant other, Peterson, sometime around 2009. *Id.* at 104. Peterson's on-again, off-again sexual partner, Hinchy, became pregnant with Peterson's child in 2009, around the time Peterson also learned he'd contracted genital herpes. *Id.* Withers looked up Hinchy's prescription profile in Walgreen's computer system and eventually Peterson exchanged texts with Hinchy claiming to have a printout about her birth control prescription. *Id.* A loss prevention specialist determined that this resulted in a HIPAA/privacy violation, and Withers had to take HIPAA retraining in addition to receiving a written warning. *Id.* at 105.

[262] *Id.* at 107–08.

[263] *Id.* at 109–10.

[264] *Id.* at 106.

privacy and confidentiality, this will better compensate victims and make independent torts more practicable.

In sum, the Ohio approach avoids the most preemption problems, and will also allow courts to carefully craft their own solutions that can be more stringent and more protective than the federal laws. Thus, this Note recommends that courts strongly consider adopting a modified Ohio approach, namely an independent tort approach with high levels of damages, an expanded category of individuals who can be liable for medical privacy violations, an expanded definition of "unauthorized disclosures," and respondeat superior liability. Because of preemption concerns, this will help courts ensure that their tort approaches fall into the "more stringent" category. However, lower courts' analyses likely need Supreme Court guidance on preemption, so, as discussed below, it is important for the Supreme Court to accept certiorari on a HIPAA preemption case.

E. *The Supreme Court Should Rule in Favor of Non-HIPAA-Influenced Torts, or Alternatively Rule in General on the HIPAA Preemption Issue*

Regardless of which approach is correct, the United States Supreme Court[265] needs to rule on how HIPAA impacts these state solutions, especially the tort claims. As seen above, different state courts vary in their approaches to the interaction between state and federal rules regarding medical privacy. This is specifically the situation HHS intended to remedy by promulgating the Privacy Rule.[266] Congress has been seemingly unwilling or unable to amend HIPAA (and HHS has not created new regulations as such) to clarify whether or not HIPAA may be used in private actions.[267] Also, based on the recent state court cases regarding this issue, it appears states will continue to create their own, diverging standards.[268]

---

[265] The Ohio Supreme Court should consider taking such a case as well. Providing guidance to Ohio courts on their unclear and somewhat conflicting approaches could serve as a beneficial guidepost in attempting to implement a non-HIPAA-based tort approach.

[266] *See* Standards for Privacy, *supra* note 46, at 82,463 ("Rules requiring the protection of health privacy in the United States have been enacted primarily by the states. While virtually every state has enacted one or more laws to safeguard privacy, these laws vary significantly from state to state and typically apply to only part of the health care system.").

[267] At this time, there do not appear to be any proposed bills or regulations clarifying this issue. Furthermore, with 2017 campaign promises of eliminating two old regulations for every new regulation, it seems unlikely new regulations about this will be promulgated any time soon. *See* Brian Naylor, *Vowing To Roll Back Regulations, Trump Faces Uphill Task*, NPR (Nov. 25, 2016), https://www.npr.org/2016/11/25/503127009/vowing-to-roll-back-regulations-trump-faces-uphill-task (on file with *Ohio State Law Journal*).

[268] *Compare* Sheldon v. Kettering Health Network, 40 N.E.3d 661, 672 (Ohio Ct. App. 2015) (rejecting the use of HIPAA in negligence per se and as a standard of care in negligence claims), *with* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 49 (Conn. 2014) (allowing HIPAA to inform the standard of care in negligence claim). While this Note advocates the tort-based approach, state-developed statutory approaches are

By ruling on whether or not HIPAA can influence state torts, and if so in what fashion, the Supreme Court could help fulfill the purposes of HIPAA's Privacy Rule. These purposes are protecting and enhancing consumer rights, improving health care quality "by restoring trust in the health care system," and "improv[ing] the efficiency and effectiveness of health care delivery by creating a national framework . . . that builds on efforts by states, health systems, and individual organizations and individuals."[269] As states continue to diverge from one another by creating differing standards, trust is lost between state lines, a national framework is undermined, and patient rights are left in an uncertain position.[270]

The importance of medical privacy is generally unquestioned,[271] and the Supreme Court itself has recognized the importance of protecting personal health information.[272] For example, in *Whalen v. Roe*, the Court noted there is a constitutionally protected interest in privacy, which includes "the individual interest in avoiding disclosure of personal matters."[273] Medical privacy serves important interests, including the public interest in ensuring individuals can get appropriate and honest physical and mental healthcare, which is "a public good of transcendent importance."[274] In a world where extremely private information like one's genetic profile can be available online, privacy protections are more important than ever.[275]

---

likely to survive the HIPAA preemption analysis as well, especially since legislatures are able to more easily tailor rules so they are more stringent/protective of patients' rights. *See, e.g.*, Hall & Nickel, *supra* note 99 (discussing Texas's more stringent medical privacy standards); *State and Federal Health Privacy Laws*, ATT'Y GEN. TEX., https://www.texasattorneygeneral.gov/cpd/state-and-federal-health-privacy-laws [https://perma.cc/KU3L-4UGP] ("[T]he Texas Medical Records Privacy Act provides additional protections to consumers. The Act is broader in scope than HIPAA because it applies not only to health care providers, health plans and other entities that process health insurance claims but also to any individual, business, or organization that obtains, stores, or possesses PHI as well as their agents, employees and contractors if they create, receive, obtain, use or transmit PHI."). What this Note answers, however, is how states without such statutes (or those with statutes that still allow for other common law approaches) should judicially approach medical privacy violations.

269 *See* Standards for Privacy, *supra* note 46, at 82,463.

270 Uniformity concerns existed even in the year 2000. Opinion, *Strong Protection for Medical Privacy*, N.Y. TIMES (Dec. 27, 2000), http://www.nytimes.com/2000/12/27/opinion/strong-protection-for-medical-privacy.html (on file with *Ohio State Law Journal*) ("The new rules set a national minimum standard but do not override stricter state laws limiting disclosure of information about such conditions as AIDS, cancer and mental illness. That will leave health plans the costly task of meeting many different standards, potentially driving up premiums that are already soaring.").

271 *See supra* Part II.A.

272 *See* Whalen v. Roe, 429 U.S. 589, 598–99 (1977); *see also* Standards for Privacy, *supra* note 46, at 82,464–65.

273 *Whalen*, 429 U.S. at 598–99.

274 Jaffee v. Redmond, 518 U.S. 1, 11 (1996).

275 *See* Standards for Privacy, *supra* note 46, at 82,465.

Despite ever-changing technology and new threats, there has been no new national move to clarify standards and improve continuity among states with regard to HIPAA. So far, many courts have also been generally unwilling to take such cases.[276] In 2013, the United States Supreme Court actually denied certiorari in a case about HIPAA-influenced torts.[277] In *R.K. v. St. Mary's Medical Center, Inc.*, Plaintiff R.K was admitted as a psychiatric patient and "disclosed confidential personal information that he had not previously disclosed to anyone, including his estranged wife."[278] He did not authorize the hospital to disclose any information about his condition or hospitalization to anyone, but hospital employees still "improperly accessed his medical records" containing his psychological information and disclosed this confidential information to his wife and her divorce attorney.[279] R.K. sued the hospital for many negligence-based claims, as well as "breach of confidentiality, invasion of privacy, and punitive damages."[280]

The hospital claimed these were merely disguised HIPAA claims, which the lower court agreed with and dismissed "based upon HIPAA preemption."[281] The state's Supreme Court of Appeals, however, found that "HIPAA [did] not preempt state-law causes of action for the wrongful disclosure of health care information."[282] The court also noted, without explicitly holding, that "contrary to finding state common-law claims preempted by HIPAA, several courts have found that a HIPAA violation may be used either as the basis for a claim of negligence *per se*, or that HIPAA may be used to supply the standard of care for other tort claims."[283]

---

[276] *See, e.g.*, St. Mary's Med. Ctr., Inc., v. R.K., 133 S. Ct. 1738 (2013) (mem.) (denying certiorari to a lower court decision authorizing HIPAA-based torts); Young v. Carran, No. 2008-SC-000862-D, 2009 Ky. LEXIS 592 (Ky. Aug. 19, 2009) (denying discretionary review of lower decision, which rejected argument that state statute codifying common law negligence per se actually created a state cause of action for a HIPAA violation), *denying cert. to* Young v. Carran, 289 S.W.3d 586, 588 (Ky. Ct. App. 2008); Webb v. Roberson, No. W2012-01230-SC-R11-CV, 2013 Tenn. LEXIS 1085 (Tenn. Dec. 23, 2013) (denying certiorari to lower court decision finding state law was not preempted by HIPAA). On a broader note, in 2008 the U.S. Supreme Court was asked to grant certiorari in a case regarding a HIPAA-influenced standard of care. Petition for a Writ of Certiorari at 54–55, Spaeth v. Cherokee Ctr. for Change, Inc., 555 U.S. 883 (2008) (No. 08-56) ("[Urging] this Honorable Court . . . to grant Certiorari in this matter, such that: . . . The federal Health Insurance Portability and Accountability Act ("HIPAA") can be consistently interpreted and applied across States, ensuring every United States Citizen[] is afforded their Constitutional rights (U.S. & State) to equal protection of their protected health information."). However, the petition was denied. *Spaeth*, 555 U.S. 883 (mem.).

[277] *St. Mary's Med. Ctr.*, 133 S. Ct. 1738.

[278] R.K. v. St. Mary's Med. Ctr., Inc., 735 S.E.2d 715, 717 (W. Va. 2012).

[279] *Id.*

[280] *Id.* at 718.

[281] *Id.* at 718–19.

[282] *Id.* at 721.

[283] *Id.* at 723.

The medical center petitioned for certiorari on February 13, 2013.[284] In the petition, the medical center claimed that the common-law torts were an "obstacle to the full purposes and objectives" of HIPAA, and should thus be preempted.[285] The lower court's decision allowed West Virginia to provide a remedy for HIPAA violations that Congress never intended, which was contrary to HIPAA.[286] The medical center rejected the notion that this overlap was acceptable because both HIPAA and the common law complemented one another and discouraged improper disclosures.[287] Instead, it argued HIPAA was intended to "create a national framework for the disclosure of personal health information," which would become unworkable with these common law torts.[288]

Thus, in denying this petition for certiorari, the Supreme Court passed on the opportunity to clarify federal preemption standards, uphold the federal floor established by HIPAA, and help reestablish uniformity among medical privacy actions. This does not serve to clarify standards and will likely only work to increase litigation, which may in turn increase confusion.

If this area of law is to have any type of clarity or national standard, the Supreme Court needs to accept a case and decide on the preemption issue. If it decides to allow HIPAA-based torts, this will permit the states to develop their own expertise on HIPAA violations and perhaps increase federal–state cooperation in analyzing such issues. Rather than giving vague rulings that dance around HIPAA standards, this will encourage courts to actually address violations in tandem with federal law.

If, on the other hand, the Court rules against HIPAA-based torts, as this Note recommends, this will permit states to move away from continuous analysis of HIPAA standards and focus more on their individual state needs. This can allow for more specific regulation, and might actually encourage states to adopt statutory standards rather than relying on the unclear and complex HIPAA requirements.

Either way, a Supreme Court ruling will allow states to finally start achieving justice and compensation for victims of medical privacy violations. As it stands now, individuals' privacy rights vary between the states and are on

---

[284] Petition for Writ of Certiorari, *St. Mary's Med. Ctr.*, 133 S. Ct. 1738 (No. 12-1007). The question presented was "[w]hether Respondent's common-law tort claims, which are premised upon an alleged wrongful disclosure of personal health care information, are preempted by the Health Insurance Portability and Accountability Act of 1996." *Id.* at i.

[285] *Id.* at 6–7.

[286] *Id.* at 8–9 (implying that these claims were essentially private causes of action under HIPAA).

[287] *Id.* at 9.

[288] *Id.* at 10. The following example was given: While medical centers normally receive requests for medical records from law enforcement, their disclosures are based on HIPAA, which says that covered entities may disclose in such situations. *Id.* However, with the possibility of common law suits, medical centers could face negligence or privacy torts for this type of HIPAA compliance if the common law was more stringent than HIPAA. *Id.* at 11.

an uncertain path. A person can recover damages in one state, but not another, for the same type of violation that Congress has previously attempted to prevent. Through clarification, this variation and uncertainty can hopefully be erased, and victims can at least be compensated for their real and tangible losses.

VI. CONCLUSION

Medical records are often sensitive, deeply personal, and damaging when exploited. When their medical information is improperly disclosed, individuals can face harrowing situations, such as job loss, reputational harm, embarrassment, and shame. It is no wonder that Congress sought to create comprehensive medical privacy reform when it passed HIPAA. However, as HIPAA enforcement has continued on a slow and non-sanction-based path, victims of medical privacy violations have been left without this supposed federal shield. In response to this problem, states have undertaken to craft their own solutions.[289] However, these solutions vary across state lines and provide unequal protections for important rights.

Addressing privacy violations via tort law has been one of the most common approaches, but there is now a split in how states approach this. Some allow HIPAA to influence their torts,[290] and some believe HIPAA-influenced torts are merely a disguise for a forbidden cause of action under HIPAA itself.[291] While there are still questions as to exactly how HIPAA preemption works in this context, especially because these are relatively new developments, the non-HIPAA-influenced tort approach seems to avoid the most preemption problems while providing greater patient protections.

For this reason, should the Supreme Court finally accept a HIPAA preemption case, it should rule in favor of this type of tort. More generally, the Supreme Court should accept a HIPAA preemption case in the first place to create uniformity and reestablish what the national framework is. As medical privacy litigation will likely continue its increase alongside new medical data technologies, this would help set expectations for providers and patients, and reaffirm the importance of medical privacy in American law.

---

[289] Some state solutions existed prior to HIPAA, and some are now influenced by HIPAA. *See supra* Part IV.B.

[290] *See* Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 49 (Conn. 2014) (allowing HIPAA to inform the standard of care in negligence cases).

[291] *See* Sheldon v. Kettering Health Network, 40 N.E.3d 661 (Ohio Ct. App. 2015) (cautioning that the *Biddle* tort should not be construed as a de facto private right of action under HIPAA).